AD________________

Award Number: DAMD17-01-C-0048

TITLE: Defense Healthcare Information Assurance Program(DHIAP) Phase III

PRINCIPAL INVESTIGATOR: Archie Andrews

CONTRACTING ORGANIZATION: Advanced Technology Institute
North Charleston, S.C. 29148

REPORT DATE: October 2003

TYPE OF REPORT: Final

PREPARED FOR: U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

DISTRIBUTION STATEMENT: Approved for Public Release;
Distribution Unlimited

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** October 2003	**3. REPORT TYPE AND DATES COVERED** Final(30 Ju71 2002 - 31 Aug 2003)

4. TITLE AND SUBTITLE
Defense Healthcare Information Assurance Program(DHIAP)
Phase III

5. FUNDING NUMBERS
DAMD17-01-C-0048

6. AUTHOR(S)
Archie Andrews

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Advanced Technology Institute
North Charleston, S.C. 29148

E-Mail: andrews@aticorp.org

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 Words)

This report covers activities and accomplishments of Phase III of the Defense Healthcare Information Assurance Program (DHIAP) for the period 30 July 2001 to 30 July 2003. Phase III tasks include: Technical Management, Deploy OCTAVE, OCTAVE Tools, OCTAVE Comparative Analysis, and Biometric Authentication Prototype. The Deploy OCTAVE effort developed and delivered DoD-specific training in use of the OCTAVE Methodology for conducting risk assessments. OCTAVE Tools developed two forms of automated support for the DoD's use of OCTAVE—a PC-based OCTAVE Automated Tool (OAT) to guide site Medical Information Security Response Teams (MISRTs) through execution of OCTAVE while capturing data and generating interim and final reports, and a Risk Database (RDB) for centralized capture and analysis of site-level OAT data. OCTAVE Comparative Analysis produced reports comparing the OCTAVE process and outputs to other MHS requirements, specifically to execution and results of DITSCAP, requirements of the HIPAA Security/Privacy Standards, JCAHO requirements, and requirements of the NIST Best Practices for Information Security (NIST SP 800-30). The Biometric Authentication Prototype effort developed and piloted a server and workstation outfitted with biometric authentication technologies (fingerprint, face, iris, and voice) and reported on utility/desirability of various biometric authentication approaches in medical environments with diverse characteristics.

14. SUBJECT TERMS
Information Security, Information Technology, Information Assurance, Computer Security, Risk Analysis, Risk Assessment, OCTAVE, OCTAVE Training, Biometric Authentication, HIPAA Privacy, HIPAA Security, JCAHO, DITSCAP, NIST Best Practices, NIST SP-800-30, MISRT Training

15. NUMBER OF PAGES
173

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** Unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

FOREWORD

Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the U.S. Army.

(X) Where copyrighted material is quoted, permission has been obtained to use such material.

(X) Where material from documents designated for limited distribution is quoted, permission has been obtained to use the material.

(X) Citations of commercial organizations and trade names in this report do not constitute an official Department of the Army endorsement or approval of the products or services of these organizations.

( ) In conducting research using animals, the investigator(s) adhered to the "Guide for the Care and Use of Laboratory Animals", prepared by the Committee on Care and Use of Laboratory Animals of the Institute of Laboratory Animal Resources, National Research Council (NIH Publication No. 86-23, Revised 1985).

( ) For the protection of human subjects, the investigator(s) have adhered to the policies of applicable Federal Law 32 CFR 219 and 45 CFR 46.

( ) In conducting research utilizing recombinant DNA technology, the investigator(s) adhered to current guidelines promulgated by the National Institute of Health.

Andrews

Principal Investigator

09/30/2003

Date

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Addendum to Final Report: DHIAP Phase III

TABLE OF FIGURES

TABLE OF TABLES

1 Introduction

The Defense Healthcare Information Assurance Program (DHIAP) is a multi-year, multi-phase program to develop and apply tools and techniques that provide an evaluation of current networks and systems and address necessary doctrine, infrastructure, training, programmatic, and technology issues to improve information assurance for Department of Defense (DoD) medical treatment facilities (MTFs). This Final Report reviews efforts of Phase III of the program.

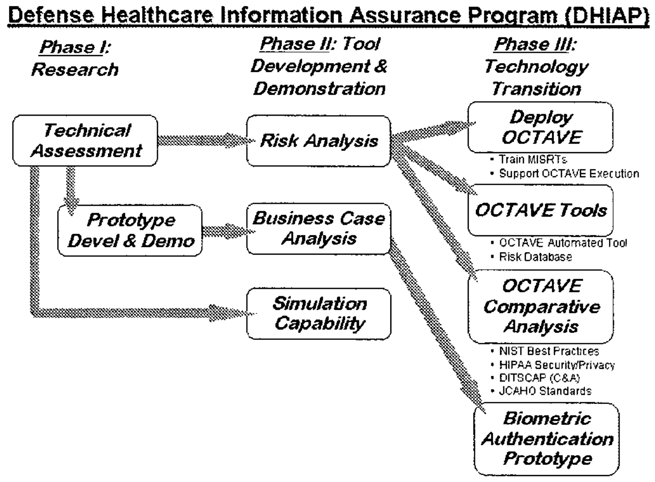


Figure 1 - Overview of DHIAP Efforts

Figure 1 portrays the progression of activities through the three phases of DHIAP. Phase I was research-focused, and Phase II developed, demonstrated, and analyzed technologies that Phase I results proved to be key to improving information assurance for the Military Health System (MHS). Phase III developed enhancements and support mechanisms for the Phase II research products, transitioned them to MHS, and performed pertinent research and analysis.

1.1 Background: Overview of DHIAP Phases I and II

The Phase I activities began with evaluating the vulnerability of patient information in the Military Healthcare System and identifying the types of activity that would be required in the future to protect it. Phase I also developed solutions for addressing some of these vulnerabilities, in one case developing and transitioning to operational use a prototype technology to protect against unauthorized information access by a remote dial-in system user, and in other cases documenting with white papers the role, requirements and characteristics of three additional examples of information assurance issues affecting military MTFs.

Phase II activities focused on enhancing the Phase I research products so they could be used by military organizations of all types to protect their information resources. Phase II included three areas of research: developing a Risk Analysis (RA) methodology and refining it based on lessons learned and results of piloting it at MTF sites; developing a Business Case Analysis (BCA) methodology and refining it by conducting BCAs on selected techniques used in medical facilities to ensure protection of healthcare information; and developing a Simulation Capability for modeling changes in approaches to securing distributed systems and assessing the effects of each hypothetical approach.

The goal of the Phase II efforts was to advance tools developed in Phase I-II research to a level appropriate for transition to operational entities throughout the military (from individual MTFs to headquarters and other higher echelon organizations) and to encourage their use in ongoing efforts to improve the information assurance posture of the military healthcare system. Appendix 1 provides a brief summary (adapted from the DHIAP Phase I and II Final Report [FNL]) of the work and accomplishments of Phases I and II.

1.2 DHIAP Phase III

DHIAP Phase III consisted of four interdependent technical projects: Deploy OCTAVE, OCTAVE Tools, OCTAVE Comparative Analysis, and Biometric Authentication Prototype. The Technical Management effort coordinated and supported the work of those tasks. The Phase III tasks are summarized below.

1.2.1 Technical Management

Management of Phase III work included coordinating with senior members of the project teams to plan tasks, schedules, and budgets, monitoring project progress, managing project resources, and providing USAMRAA and TATRC with regular reporting of project and program accomplishments and expenditures. It also involved preparing command- and operational-level briefings as requested by the Contracting Officer's Technical Representative (COTR).

1.2.2 Deploy OCTAVE

Work to deploy the DHIAP-developed Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE[SM]) Method throughout the DoD healthcare community consisted of two major subtasks: *Train MISRTs* (Medical Information Security Readiness Teams) and *Support OCTAVE Execution.* Completion of the effort provided DoD with an OCTAVE-trained workforce and an effective support infrastructure for continuing use of the OCTAVE Method.

1.2.2.1 Train MISRTs

DHIAP OCTAVE training activities began with the Team developing a 1½-day training course (based on the standard 3-day approach to OCTAVE training) that was customized to DoD/MHS priorities and needs. The initial OCTAVE training was delivered at the "TMA HIPAA Summit 2001" to MISRTs from the DoD's sixteen largest medical centers worldwide. Next, between May and August 2002, the Team extended the MHS OCTAVE rollout by conducting twenty training seminars at locations around the world that were attended by MISRTs from over 170 DoD medical centers and all TRICARE regions.

1.2.2.2 Support OCTAVE Execution

To facilitate rapid execution of risk assessments at MHS facilities and broad acceptance of OCTAVE, the DHIAP Team established a base of support known as the OCTAVE Information Center (OIC). The Team used the OIC to provide both customized guidance and general information to MISRTs. Support provided through the OIC included: corresponding directly with trained MISRTs via e-mail (and follow-on telephone conversations as appropriate); referring the MISRTs' questions to the DHIAP Team member with the background most appropriate for addressing each subject; monitoring the Team's advice to MISRTs to ensure adequacy and accuracy of the response; and posting as "Frequently Asked Questions" (FAQs) any advice that might have broad applicability to other MISRTs. The Team used an OIC function known as the "DHIAP Trainers-Only area" to log queries/responses they participated in and to post other information they obtained about MTFs' OCTAVE execution status, etc.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University. Development of OCTAVE was partially sponsored by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD 17-99-C-9001 and DAMD17-01-C-0048, Phases I-II and Phase III of the Defense Healthcare Information Assurance Program (DHIAP).

1.2.3 OCTAVE Tools

OCTAVE Tool development consisted of two interrelated design, development, and rollout subtasks—*OCTAVE Automated Tool (OAT)* and *Risk Database (RDB)*. The OAT is a PC-based system designed to support site MISRTs during execution of OCTAVE; the RDB is a centralized database capability designed to gather and support analysis of the OAT data from multiple facilities (e.g., analysis of input from all facilities of one service, all facilities from a region, all MHS facilities, etc.). Completion of the project provided DoD with automated support for MTF-level execution of OCTAVE and, in order to identify and resolve issues that were being experienced system-wide, a tool to support higher echelons' analysis of aggregate OCTAVE results.

1.2.3.1 OCTAVE Automated Tool (OAT)

The OCTAVE Automated Tool (OAT) was developed by the DHIAP Team as standalone PC-based software to streamline the record keeping and report generation activities of an OCTAVE risk assessment. The OAT was designed to support the OCTAVE assessment's scribe functions of recording data generated during each of the OCTAVE workshops, manipulating it as needed to be input to upcoming workshop activities, and preparing the OCTAVE interim and final reports. In addition, OAT's design provided additional user support through its use of unique tabs for each OCTAVE decision and data entry step, sequencing of activities, use of screens and pop-up windows to provide instructions and hints, and links to the appropriate sections of the *OCTAVE Method Implementation Guide, Version 2.0* [OM2].

DHIAP pilots of the OAT proved that it is effective in guiding OCTAVE-trained users through the steps of the OCTAVE process, providing the references, support, and hints that are appropriate for each step. On a technical level, the OAT implements the information model guidelines for capturing data and generating essential reports that are consistent with the RDB, provides a Graphical User Interface (GUI) for the entry (with quality assurance checks incorporated into the data collection process) and display of OCTAVE assessment data, retains OCTAVE data in a local data store, and securely transfers data from the local PC to the centralized RDB.

1.2.3.2 Risk Database (RDB)

The RDB was developed by the DHIAP Team to be a central repository for data acquired through sites' execution of OCTAVE. It was designed to permit higher echelons to gain a system-wide view of the risks facing the MTFs. The RDB provides extensive data selection and query capabilities to support the types of data analysis and consolidation required to meet this goal. When fully implemented by MHS or other military organizations, the RDB will enable investigation of systemic and global information assurance risks faced by MTFs and establish the basis for developing solutions that could dramatically improve the safety and security of sensitive data throughout the MHS.

1.2.4 OCTAVE Comparative Analysis

The goal of the DHIAP Comparative Analyses was to determine whether execution of an OCTAVE risk assessment and/or implementation of its results might help MTFs comply with requirements placed on them by external organizations. The DHIAP Team analyzed the OCTAVE Method and its work products in relation to the following processes and regulations that significantly affect MHS facilities:

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DIT];
- Security Standards [SEC] and Privacy Standards [PVC] of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [HPA];
- Accreditation Standards of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) [JCA]; and
- Security Best Practices as reflected in the NIST Risk Management Guide for Information Technology Systems/NIST SP 800-30 [NST].[1]

The reports that resulted from this research provide guidance on how OCTAVE relates to the work efforts and work products associated with meeting requirements of these processes and regulations. In some cases, the reports provide guidance on how OCTAVE efforts might be coordinated with efforts to satisfy these other external requirements.

Another effort of this task was to develop recommendations for tailoring the "classic" OCTAVE Method to be more directly applicable to DoD-MHS environment and issues. The Team completed this effort by preparing a list of recommendations based on knowledge the Team acquired from conducting MHS' OCTAVE training, providing support to site MISRTs through the OCTAVE Information Center, and identifying OCTAVE's potential to complement an MTF's DITSCAP, HIPAA, JCAHO, and information security best practices requirements.

1.2.5 Biometric Authentication Prototype

To study the effects of using various modes of biometric authentication in an operational MTF environment, the DHIAP Team designed a prototype biometric authentication system and conducted MTF trials of its use. Building upon the findings of the DHIAP Phase II Business Case Analysis (BCA), Effective Authentication in a Medical Environment [EAU], the task tested the following hypotheses:

H_{O1}: Users find no biometric method of authentication preferable in the operational environment

H_{O2}: No biometric method of authentication is suitable to replace passwords

Project efforts began with building a prototype authentication system that offered several alternative techniques for authentication (e.g., iris scan, fingerprint, facial identification, and voice identification) and collected data on user attempts to authenticate using the system. The effort concluded by publishing report on the utility and limitations of current and emerging biometric technologies when applied to a medical treatment facility's operational environment.

[1] The original Phase III Technical Development Plan [TD3] called for performing this comparison against RFC-2196-The Site Security Handbook (a guide to developing computer security policies and procedures for sites that have systems on the Internet, available from http://www.faqs.org/rfcs/rfc2196.html). The plan was changed with COTR approval during the first year of Phase III.

2 Body

Healthcare information systems manage access to enormous amounts of sensitive but unclassified information. While the MTF operational environment requires efficient and effective access to the data when and where it is needed, various regulations require that the information be handled in ways that protect its privacy, confidentiality, and integrity. The research activities of DHIAP Phases I and II, conducted between October 1998 and May 2001, developed technologies and research reports to support the Military Healthcare System in addressing this information protection challenge. Phase III activities, conducted between July 2001 and August 2003, were designed to transfer these technologies throughout MHS and provide additional assistance in the forms of support mechanisms and research reports that would help MHS and its MTFs maximize the benefit derived from using the technologies.

Each of the tasks outlined in the Introduction to this report is covered in greater detail in this section. For each project task, "Methods/Discussion" summarizes the methods adopted to perform the work, along with a discussion of any issues, problems, or major discoveries that arose during the period, and "Results" summarizes the task's results relative to the goals and plans outlined in the Phase III Technical Development Plan.

2.1 Technical Management

The Technical Management task consisted of two subtasks, *Initiate Phase III Work* (awarded via letter contract for the time period, 30 July – 13 September 2001) and *Manage DHIAP Activities*, which provided guidance for all Phase III technical efforts from 30 July 2001 through 15 August 2003.

2.1.1 Initiate Phase III Work

Methods/Discussion: The focus of initial Phase III Technical Management efforts in August-September 2001 involved planning, preparing for, and conducting OCTAVE Training for the September 2001 "TMA HIPAA Summit 2001." Beginning in early August 2001, DHIAP leaders worked with TATRC and TRICARE Management Activity (TMA) representatives to coordinate DHIAP Team efforts for the Summit. DHIAP leaders organized and managed development of training and support materials for the Summit's pilot of a DoD-tailored version of the OCTAVE Training course that DHIAP Phase II had developed. (The DoD customizations consisted of a detailed script for conducting each OCTAVE workshop, as well as certain DoD-specific visual aids and student handouts.) DHIAP leaders worked with TATRC to acquire and arrange for delivery of training materials (e.g., copies of the OCTAVE manuals and electronic versions of CDs, posters, etc.). DHIAP leaders arranged and facilitated a Team meeting in late August to finalize plans and staffing for conducting the Summit's four concurrent two-day sessions of OCTAVE Training. Throughout the period, they ensured that all work assignments associated with preparing for the Summit were completed on schedule. Additional information on the methods and results of the HIPAA Summit Training effort is provided in the sections below on "Develop OCTAVE Training for HIPAA Summit" and "Deliver OCTAVE User Training at DoD HIPAA Summit."

Also during the pre-award period, DHIAP leaders began drafting the Phase III Technical Development Plan (TDP), its descriptions of tasks, resource assignments, work breakdown schedules, lists of deliverables and issues/dependencies, and estimates of projected travel and equipment needs. The effort began with a Team meeting in mid-September 2001 to develop details that would become the TDP contents.

During this timeframe, the DHIAP COTR learned that it would be necessary to increase the Team's involvement in conducting OCTAVE training for MISRTs from the original plan of four sessions to a new plan for twenty sessions (some in overseas locations). The DHIAP leaders determined labor, travel, and printing/shipping costs associated with the expanded effort and adjusted the Phase III budget, workload estimates, and work schedules to accommodate this need. DHIAP leaders reviewed TDP contents with TATRC in mid-October 2001, released the next TDP draft released in early November 2001, and began working with TATRC and USAMRAA to obtain formal approval of the changes associated with the training revisions.

TATRC requested that the TDP include OCTAVE Automated Tool, Risk Database, and Biometric Prototype technical specifications and requirements that had been confirmed in a mid-November 2001 DHIAP Team meeting. The DHIAP leaders updated the TDP to include that documentation and submitted the updated TDP to the CO and COTR on 5 December 2001 and again on 20 December 2001.

Early in 2002. TATRC determined that there would be schedule changes for two portions of the work plan as reflected in the TDP. To accommodate MHS needs, the start of MISRT training was to be shifted from February to May; also, in response to MHS/MTF requests, the OCTAVE Automated Tool's availability for field use was to be accelerated. DHIAP leaders worked with TATRC to develop revised schedules for these efforts and the other Phase III efforts that they affected, publishing an updated version of the TDP on 11 March 2002.

Result: The TATRC/DHIAP Team efforts to support the TMA HIPAA Summit 2001 were highly successful. Representatives of the largest Medical Treatment Facility (MTF) in each TMA region were trained there, along with TMA Lead Agents and many other individuals representing each branch of the services and some specialized organizations within the services. Many of the DoD-specific training support guidelines and course materials that were piloted at the Summit remained "as-is" for future Phase III training use, while some other materials served as the basis for enhancement later in Phase III in the "Deploy OCTAVE" task activities.

Throughout the extended TDP development timeframe, DHIAP leaders and Team members used the TDP as the guideline for execution of Phase III tasks. COTR approval of the DHIAP Phase III Technical Development Plan [TD3] (included as **Error! Reference source not found.**) was provided on 21 March 2002.

2.1.2 Manage DHIAP Activities

Methods/Discussion: The DHIAP Principal Investigator (PI) oversaw execution of all DHIAP Phase III work, monitoring project execution against the TDP commitments for budget, schedule, and technical goals, and monitoring changes in the project risk environment. Working closely with other DHIAP leaders, the PI evaluated progress of project work efforts, production of deliverables, and use of resources. As appropriate, the PI worked with DHIAP Team members and the COTR to define and execute corrective action. As a part of overseeing project execution, the PI and DHIAP leaders ensured that Technical Management staff made the necessary arrangements for travel, meeting support, and preparation of materials needed for planned activities such as the training sessions.

Early in the second half of 2002, it was evident that the MHS-driven schedule changes had driven the need to change timing of some other project tasks. For example:

- Deferral of OCTAVE training by four months meant that tasks such as "Provide Support to MISRTs" and the portion of "Develop Train-the-Trainer Seminar/Deliver Instructor Training to DoD" that was to provide a "tested" training course to a DoD organization should be deferred so they would still be conducted following the completion of training.
- Some tasks of OCTAVE Automated Tool and Risk Database development and testing, which were to use the results of field execution of site OCTAVEs, should be deferred until late 2002 when site-generated data would be available.
- If the Risk Database development and testing tasks were not deferred, the Risk Database would have to be delivered to DoD without benefiting from lessons learned by testing with field-generated OCTAVE Automated Tool data.

Therefore, the PI began working with the COTR to determine the best approach to deferring some project efforts that would be more appropriately conducted in December 2002 and later. The PI prepared a summary documenting the work that had been completed on schedule, defining reasoning and revised completion dates for the project tasks to be deferred, and documenting additional work that the COTR agreed should be performed during the period of the proposed extension. The PI submitted a request for a no-cost extension and a revised budget to USAMRAA on 10 December 2002. DHIAP leaders continued to execute the Phase III work plan as appropriate to the changed operational environment, and USAMRAA approval of the extension and work plan revisions was received on 22 January 2003.

Result: Throughout Phase III, the PI and the DHIAP leaders directly oversaw development of project plans and design/development of deliverables. As changing MHS and TATRC priorities drove the need to change the schedule for providing certain project deliverables, they worked with TATRC to make the most appropriate changes to staffing plans and execution timeframes. The leaders conducted interim reviews with TATRC of the various products of Phase III efforts, and they ensured that interim and final results of the various activities meet TATRC's and the Team's own expectations for quality, timeliness, and cost-effectiveness.

The PI's request to extend Phase III work through August 2003 and USAMRAA's favorable response enabled the DHIAP Team to provide all deliverables defined in the original TDP in revised timeframes that were more appropriate to MHS' priorities and schedules.

(The "Revised Program Plan—DHIAP III, 9 December 2002" [TDR] is included as Appendix 5 – Revised Program Plan—DHIAP III, 9 December 2002.)

In addition, the Team was able to provide extra benefit to DoD in the form of an extended period of support to OCTAVE users at MTFs, extended and expanded field trials of the OCTAVE Automated Tool, and an OCTAVE training package that incorporates knowledge gained from the MHS-deferred cycle of training seminars.

Another important benefit that accrued from the Phase III extension was performance of some newly conceived tasks that were important additions to DHIAP technical efforts. One of these tasks involved performing detailed security testing on the OCTAVE Automated Tool and Risk Database. The other task produced these tools' documentation elements according to a standard and in a format appropriate for submission to a Designated Approving Authority (DAA) for a Certification & Accreditation (C&A) designation of Interim Authority to Operate (IATO).

2.2 Deploy OCTAVE

The task to deploy OCTAVE consisted of two subtasks, *Train MISRTs on OCTAVE* and *Support OCTAVE Execution.* The OCTAVE Training effort had two major activities—one to develop training materials/schedules and conduct training for MISRTs from all MHS MTFs, and the other to develop an OCTAVE Train-the-Trainer course and deliver it to a TATRC-identified service organization that would assume ongoing DoD responsibility for providing OCTAVE training. The OCTAVE Support effort included two interdependent activities—one provided direct support to trained MISRTs as they conducted their sites' OCTAVE risk assessments, and the other developed and implemented a web-based OCTAVE Information Center (OIC), used the OIC as the mechanism for providing OCTAVE execution support to MISRTs, and delivered the operational OIC to DoD for continuing use.

2.2.1 Train MISRTs on OCTAVE

Training the appropriate medical center staff members (i.e., the MISRT appointed by the MTF) to conduct OCTAVE risk assessments is expected to produce MHS-wide acceptance and use of the OCTAVE Method and, by extension, effective integration of risk analysis into the information assurance management activities of DoD MTFs. In this task, the DHIAP team members appointed to serve as "DHIAP Trainers" developed materials needed for conducting the DoD-customized training of site MISRTs, completed the logistics to conduct a world-wide training effort, and, finally, conduct twenty seminars at major DoD regional centers worldwide to that train MISRTs from over 170 MTFs on use of the OCTAVE Method.

2.2.1.1 Develop OCTAVE Training for HIPAA Summit

Methods/Discussion: As described for the Technical Management "Initiate Phase III Work" task, the DHIAP PI met with TATRC to prepare for conducting the training, developing a preliminary plan for development of training materials and execution of training responsibilities. They identified the DHIAP Team members who serve as trainers, and they developed lists of critical short-term actions to be carried out by both DHIAP Team members and the MHS staff responsible for readying MHS and DoD to meet requirements of the new HIPAA regulations. The DHIAP Team members from TATRC, ATI, and KRM who would become the "DHIAP Trainers" met with SEI to define their approach to conducting MISRT training at the Summit, condensing course delivery into a shorter timeframe than SEI's standard approach and developing some DoD-unique aids for teaching the course (e.g., a wall chart, various student handouts, etc.).

The DHIAP Trainers studied the OCTAVE Method and developed detailed scripts for conducting each course segment of the DoD-version training program. Each trainer took ownership of one or more OCTAVE workshops, drafting a teaching script for the course segment and determining the need for any supporting student materials. The Team published the resulting scripts and distributed them to all trainers for review and enhancement. On the day preceding the TMA HIPAA Summit 2001 training, the DHIAP Trainers met to confirm details of their jointly developed approach to conducting the DoD training.

Result: DHIAP Team efforts produced a version of OCTAVE training that was customized for DoD use—briefer and more focused on healthcare issues and solutions than the standard OCTAVE training. The Team produced lesson plans for each workshop that provide detailed instruction on how to use the various sections of the OCTAVE Method Implementation Guide, Version 1.0 (OMIG) [OM1] during the session; a CD-ROM version of the OMIG for distribution to students; and other materials (e.g., a wall chart depicting sequence and purpose of OCTAVE's workshops and deliverables, student handouts, pre- and post-training surveys, etc.) that were necessary or would be helpful for delivery of OCTAVE training.

2.2.1.2 Deliver OCTAVE User Training at DoD HIPAA Summit

Methods/Discussion: Sixteen MTFs, each one the largest medical center in its TRICARE region, were selected to attend the TMA HIPAA Summit 2001 in Washington DC on 5-7 September 2001. Other TRICARE and MHS groups, such as the TRICARE regions' Lead Agents, the HIPAA Points of Contact (POCs) for each DoD service, and other individuals representing various MHS organizations and some specialized organizations within the services, were also invited to attend. The sixteen regional MISRTs that were included in the first training were selected so that they, and their OCTAVE execution experience, would be available to support other MTFs within their regions by sharing their OCTAVE knowledge and lessons learned.

Summit activities began with a one-day overview of HIPAA conducted by various TMA/MHS leaders to explain HIPAA regulations, the DoD's activities to prepare to meet HIPAA requirements, and the reasons that attendees would spend the next two days learning how to conduct risk assessments using the OCTAVE Method. On the remaining two days of the Summit, the DHIAP Trainers delivered OCTAVE User Training to the sixteen regional MISRTs and other selected individuals invited by DoD. OCTAVE training was delivered as four concurrent sessions followed, at the end of the second day, by a brief plenary session for MISRT members to exchange ideas with each other and express concerns to MHS/TMA leaders.

Result: OCTAVE training within the DoD medical health system was initiated when Medical Information Security Readiness Teams (MISRTs) from the DoD's sixteen largest medical centers were trained on OCTAVE at the DoD HIPAA Summit in Washington DC on 5-7 September 2001. In the Summit's closing plenary session, MHS leaders directed the MISRTs to initiate planning and execution of their sites' OCTAVE risk assessments as soon as possible. The DHIAP trainers used lessons learned from conducting the training to identify ways that they could improve the training program during the remaining work of this project. In addition, they established relationships with MISRT members that would prove useful during execution of the upcoming DHIAP OCTAVE support activities of helping MISRTs with execution of their risk assessments and learning the sites' OCTAVE progress/completion status.

2.2.1.3 Conduct Wide Deployment of OCTAVE (Mobilization of OCTAVE)

Methods/Discussion: The DHIAP Team worked closely with TATRC to develop a plan for Wide Deployment of OCTAVE training to MISRTs at MTFs throughout DoD. Major steps of the activity included working with TATRC (who worked directly with the services' HIPAA POCs and TMA representatives) to:

- Establish and refine a list of MTFs to participate in OCTAVE training;
- Prepare an initial draft Deployment Plan for the training, taking into account such variables as the geographic/regional distribution of MTFs designated to attend training, availability of DHIAP Trainers, conflicts with key conferences and events;
- Submit the draft Deployment Plan to TMA and Service HIPAA POCs as appropriate, obtain feedback, and modify the draft plan as needed;

- With TMA and the Service HIPAA POCs, generate an official communication to all designated MTFs requesting that the MTFs assign MISRT members and prepare to attend training; and
- Verify that appropriate training sites were reserved, MISRTs enrolled, and student travel/accommodations arranged for each seminar.

In preparation for conducting the Wide Deployment training, the Team grouped the DHIAP Trainers into three teams of two persons each. Each team included one trainer from ATI or KRM and the other from TATRC, with assignments of individuals designed to ensure that each team had one technically focused trainer and one process-focused trainer.

The DHIAP Trainers developed the materials necessary to conduct the user training as defined in the Deployment Plan. The DHIAP Team member coordinating the effort attended SEI training on Version 2.0 of OCTAVE in late January 2002 to identify changes or enhancements that would benefit the DoD's OCTAVE training course, and then used that knowledge in managing the Team's activities to enhance training materials constructed earlier for the HIPAA Summit.

The HIPAA Summit OCTAVE training course had focused on use of [OM1]. Because SEI completed the formal publishing of an updated version of OCTAVE since that training occurred, the Team decided that training development activities to prepare for Wide Deployment would support Version 2.0 of the OCTAVE Method Implementation Guide (OMIG) [OM2]. During this training development effort, the Team made extensive use of the HIPAA Summit training materials to develop materials needed to support the OCTAVE Wide Deployment training:

- a formalized DHIAP Trainers' Instructor Guide keyed to elements of [OM2],
- a corresponding Student Handout Package, and
- a DHIAP Trainers' CD.

The DHIAP Trainers' Instructor Guide contained lesson plans, key teaching points, and guidance pages for instructors. The Student Handout Package consisted mostly of worksheets that would be used during the training seminars. The DHIAP Trainers' CD contained an electronic copy of all teaching materials, a copy of the Harris STAT® Network Vulnerability Scanner Demo software, and choreographed PowerPoint slides for use during the training sessions.

To prepare to conduct training, the DHIAP Trainers met in early May 2002 for a coordination meeting/implementation briefing that covered the Deployment Plan in detail. Agenda topics included: ensuring all trainers were aware of their pre-, during, and post-training responsibilities, setting activity lead-time requirements, verifying travel requirements, and establishing tracking and reporting requirements. The meeting also addressed issues identified by various trainers, confirmed trainer availability, identified backup trainers, arranged for distribution of updates to lesson plans/instructor checklists, and confirmed responsibility for the various logistics efforts required to support execution of the Deployment Plan (e.g., coordinating with training site POCs to arrange for a training room and supplies, arranging for copies of trainer and student materials to be made and shipping them to each training location, etc.).

The Team's early estimates projected that twenty OCTAVE training seminars would be necessary to accomplish training of all designated MTFs, each seminar having a length of two days and being attended by up to eight three-person MISRTs. As MHS/TMA provided revised plans for training timeframes, schedules, and number of trainees, the Team modified appropriate details of the preliminary Deployment Plan. Each training schedule revision had the goal of reducing costs of delivering training in distant regions (e.g., West Coast, Europe, Pacific) by having the trainers deliver multiple seminars before returning to their base location. In preparation for visiting overseas sites to conduct MISRT training, DHIAP Team representatives worked during this time with TATRC to coordinate necessary clearances/Theatre Recovery Plans and attend DoD Force Protection Briefs.

During execution of the Deployment Plan (in late June 2002, following completion of six training seminars), the DHIAP Team conducted a "Mid-Training Review" teleconference with TATRC to discuss lessons learned from the initial round of training. Actions resulting from the conference included development of an additional worksheet to include in student handout for session 8 (planning). The group decided that DHIAP trainers would begin using the OCTAVE Information Center (OIC) to communicate with each other and would register on the OIC to gain appropriate experience for explaining OIC and its use during training.

Logistics support for the training effort included frequent coordination among ATI, TATRC, service POCs, and regional Lead Agents. ATI coordinated regularly with the printer about the number of OMIG and Student Handout Packages to prepare, shipping to the training sites' POCs, etc. Coordination also included arranging for copies of the CD-ROM version of the OMIG to be reproduced and shipped to the POCs at each training location. For each shipment, the effort included confirming that all OMIGs, materials, and supplies for the training session were shipped by the printer and received by the site POC, following up to make sure all other supplies and materials necessary to support training (e.g., the poster-sized enlargements of certain worksheets, projectors, supplies such as markers, tape, extension cords, etc.) were received at the training site, coordinating the times and places for OCTAVE Trainers to meet upon arrival with site POCs to review and complete final arrangements for the classes. Post-training activities included arranging either for the return of any unused OMIGs/student materials or shipment of additional materials for walk-in students.

Upon completion of OCTAVE training at each site, the DHIAP Trainers conducted wrap-up activities that included verifying/updating the list of attendees as needed, capturing any trainers' notes and lessons learned, taking an inventory of materials and supplies brought back from training sessions, and verifying accuracy of the printer's invoices for printing and shipping of the OMIG and Student Handouts. The Trainers provided feedback to TATRC following each session. Following completion of all MISRT training, the Team developed a master document identifying all OCTAVE Training attendees for use in the "Since the DHIAP developers continually coordinated OIC development and enhancement activities with TATRC technical resources to ensure compliance with known RIMR and DoD requirements, the OIC functioned effectively throughout Phase III as an application that was accessed through RIMR but housed at the offices of ATI. At the close of DHIAP Phase III, TATRC authorized continuation of ATI's direct support for the OIC by making it a part of the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

Provide Support to MISRTs" task to verify trainee identity and determine authorization for OIC registration permissions.

Result: OCTAVE training was delivered to MISRTs of all designated MTFs between 29 May and 20 August 2002. Over 600 individuals, representing over 170 MTFs from all service branches and the US Coast Guard and other MHS organizations worldwide, attended the DHIAP OCTAVE training. TATRC extended ATI's role as DHIAP OCTAVE Trainers by defining a series of eight (later reduced to four) additional training seminars in a new ATI-led program, "OCTAVE Training and Support (OTAS)."[2] Table 1 below provides a summary of the training seminars conducted during Phase III and the sites and MISRT members in attendance at each.

Table 1 - Summary of DHIAP Phase III OCTAVE Training

DATE / LOCATION OF TRAINING SEMINAR	ATTENDEES' REGION # AND FACILITY NAME
5-7 September 2002 TMA HIPAA Summit 2001 Washington DC	Region 1:Malcom Grow- Andrews AFB, Walter Reed AMC, Bethesda NNMC Region 2: Womack AMC, Portsmouth NMC Region 3: Eisenhower AMC Region 4: Keesler AFB Region 5: Wright-Patterson AFB Region 6: Wilford Hall - Lackland AFB, William Beaumont, Brooke AMC Region 9: San Diego NMC Region 10: David Grant - Travis AFB Region 11: Madigan AMC Region 12: Tripler AMC Region 13: Landstuhl AMC
29-30 May 2002 Region 6: San Antonio, TX	TMA Region 6, Reynolds ACH at Ft Sill, Darnall ACH at Ft Hood, Bayne Jones ACH at Ft. Polk, Barksdale AFB, Dyess AFB, Altus AFB, Goodfellow AFB, Tinker AFB, Laughlin AFB, Little Rock AFB, Randolph AFB, Sheppard AFB, Vance AFB, Brooks AFB, HQ AETC, Corpus Christi NH, Kirtland AFB,
6-7 June 2002 Region 2 Norfolk, VA	TRICARE Office, McDonald ACH, Kenner AMC at Ft. Lee, Langley AFB, Seymour Johnson AFB, Pope AFB, Cherry Point NH, Camp Lejeune NH, Atlantic MAC (MIClant),
11-12 June 02 Region 4 Biloxi MS	Fox ACH, Lyster ACH, Maxwell AFB, Tyndall AFB, Columbus AFB, Eglin AFB, Hurlburt Field, Pensacola NH,
10-11 June 2002 Region 13 Ramstein, Germany	Geilenkirchen AFB, Wurzburg ACH, Heidleberg MEDDAC, Aviano AB, Ramstein AB, Lajes FLD, Spangdahlem/Bitburg, HQ USAFE, Landstuhl AMC
13-14 June 2002 Region 13 Lakenheath, England	Cincusnaveur (Navy), RAF Lakenheath, Incirlik AB, Rota NH, Naples NH, Sigonella NH, London NMC (NavMedClinics UK)
10-11 July 2002 Region 1 Washington DC	Keller ACH, Dewitt ACH, Dilorenzo TRICARE HC, Kimbrough ACC, Dunham AHC, Guthrie AHC, Bolling AFB, Hanscom AFB, McGuire AFB/Ft Dix, Patuxent River NMC, Quantico NMCL, Annapolis NMCL, NMIMC MISRT Spt, NNMC/PASL
15-16 July 2002 Region 10 Sacramento CA	California Medical Detach, Beale AFB, Pacific MAC, Lemoore NH,
16-17 July 2002 Region 5 Dayton OH	Military Med. Support Office (Navy), Ireland ACH at Ft. Knox, MEDDAC, Ft. Knox, Blanchfield AMC at Ft. Campbell, Great Lakes NH, Scott AFB, HQ AMC (Scott AFB), HQ AFMC (Wright Patterson AFB)
18-19 July 2002 Region 9 San Diego CA	Naval Dental Center, Southeast, Weed ACH at Ft Irwin, Nellis AFB (Mike O'Callaghan Fed. Hosp.), Edwards AFB, Los Angeles AFS, Vandenberg AFB, Camp Pendleton NH, Twentynine Palms NH

[2] OCTAVE Training and Support (OTAS) was sponsored by the U.S. Army Medical Research and Materiel Command under Contract No. GS-35F-0288M, Order No. DAMD17-02-F-0582.

DATE / LOCATION OF TRAINING SEMINAR	ATTENDEES' REGION # AND FACILITY NAME
24-25 July 2002 Region 3 Augusta, GA	Lawrence Joel AHC, Winn ACH, Moncrief ACH, Shaw AFB, Robins AFB, Charleston AFB, Charleston NH, Beaufort NH, Martin AMC, Moody AFB, Patrick AFB, MacDill AFB, HQ ACC – Langley AFB, Jacksonville NH, Roosevelt Roads NMH, Guantanamo Bay NH,
22-23 July 2002 Region 12 Honolulu HI	Youngsan (Army), TRICARE Pacific, Atsugi BMC, Japan (Navy), TRICARE Pacific Lead Agent, Hawaii, 18th Med Command (at Camp Zama Honshu), Hickam AFB, Pearl Harbor NMC, Okinawa NH, Guam NH, Tripler AMC
6-7 August 2002 Regions 7 & 8 Colorado Springs CO	Peterson AFB, Leonard Wood ACH, Irwin ACH at Ft. Riley, Munson AHC at Ft. Leavenworth, Raymond Bliss AHC at Ft. Huachuca, Cannon AFB, 355 MDG at Davis-Monthan AFB, Ellsworth AFB, Holloman AFB, Minot AFB, Mountain Home AFB, Offutt AFB, Whiteman AFB, Hill AFB, Kirtland AFB, Buckley ANGB, F.E. Warren AFB, Malmstrom AFB, Grand Forks AFB, McConnell AFB, USAF Academy, HQ AFSPC
13-14 August 2002 Makeup Session Washington DC	Aberdeen Proving Ground, CHPPM, HQ USCG, National Naval Dental Center, Ft. Sam Houston, Ft. Sam Houston MEDCOM (HQ), Keflavik NH, Dover AFB, Bethesda NNMC, Jacksonville NH, Guantanamo Bay NH, Fox ACH at Redstone Arsenal
15-16 August 2002 Region 12 Yokota, Japan	Atsugi BMC, Japan (Navy), TRICARE Pacific Lead Agent, Hawaii, Branch Med. Clinic Sasebo (Navy), Camp Zama Honshu Japan, Andersen AFB, Kadena AB, Kunsan AB, Misawa AB, Osan AB, Yokota AB, Hickam AFB, Yokosuka NH, MCAS Iwakuni, Guam NH,
19-20 August 2002 Region 11 Seattle-Tacoma WA	WRMC (Army), Northwest Lead Agent (Army), Fairchild AFB, McChord AFB, Elmendorf AFB, Eielson AFB, Bremerton NH, Oak Harbor NH, Luke AFB,

2.2.1.4 Identify DoD Trainers

Methods/Discussion: In this task, MHS and TATRC were to identify the service organization(s) that would assume the responsibility of being the military's ongoing provider of MISRT training. When the effort had not been completed by late 2002, the DHIAP leaders included this task in the no-cost extension that extended Phase III work through August 2003. At the close of Phase III technical efforts, no arrangements had been made for a service organization to assume responsibility for ongoing MISRT OCTAVE training.

> **Result:** The Phase III TDP [TD3] had called for the service organization selected in this task to be an important participant in the next task, "Develop Train-the-Trainer Seminar/Deliver Instructor Training to DoD" so that the resulting course and its documentation would reflect the training approach and standards utilized by that organization.

2.2.1.5 Develop Train-the-Trainer Seminar/Deliver Instructor Training to DoD

Methods/Discussion: Development of OCTAVE Train-the-Trainer materials was conducted by the SEI DHIAP Team members who had authored the OCTAVE Method in Phase II. These SEI DHIAP Team members maintained communication with the DHIAP Trainers as they conducted the following activities:

- When the course development effort had produced the first version of a Train-the-Trainer course, they piloted that version in a class on 20-21 June 2002. Attendees at that session were SEI clients (representatives of a small consulting firm in western Pennsylvania that had licensed OCTAVE) and some SEI staff.

- Based on lessons learned from the pilot, they implemented improvements to the content and organization of Train-the-Trainer materials, condensing two exercises on "delivery options" into one, and adding course segments on "planning" and "instructor notes." The enhanced Train-the-Trainer course was piloted on 29-30 August 2002, again training clients (representatives of a second western Pennsylvania consulting firm and a consulting firm from Washington DC that had acquired OCTAVE licenses) and some SEI staff.
- Based on lessons learned from the second pilot, they made some minor improvements to course content and organization of the Train-the-Trainer materials (e.g., placing additional emphasis on planning and scoping an OCTAVE).

On 13-14 February 2003, the DHIAP Team training leader attended the Train-the-Trainer course for an orientation to the curriculum. SEI provided a copy of the course materials to the DHIAP Team.

Result: The DHIAP Team produced a DoD OCTAVE Train-the-Trainer Course that is consistent with the OCTAVE Method v2.0. One component of the course provides specific instruction to help trainers re-familiarize themselves with the concepts on which the OCTAVE Method was built, enhancing their ability to teach the OCTAVE Method and help users effectively tailor the OCTAVE Method to their own needs. Another component provides the trainers with techniques for handling difficult training issues. Yet another component of the course relates to delivery of OCTAVE training, teaching how to facilitate the OCTAVE Method in a variety of delivery modes and covering how to plan and scope an OCTAVE risk assessment, the range of delivery options that can be used without violating the basic principles of OCTAVE, and a number of techniques for effectively handling difficult issues. The training module provides a self-test for each course component to enable trainers to assess their ability to conduct OCTAVE training and facilitate an OCTAVE risk assessment. The agenda for the completed OCTAVE Train-the-Trainer course is shown in Table 2 below.

Table 2 - Train-the-Trainer Course Agenda

DAY 1	DAY 2
• Opening (15 min) • Introduction to Underlying Topics (60 min) • OCTAVE Criteria and Its Use (60 min) • Review of OCTAVE Method Training Materials (90 min) • Sticky Subjects, Training (90 min) • Self-Evaluation (60 min)	• Project Planning and Scoping (1 hr 45 min) • Delivery Options (1 hr 45 min) • Sticky Subjects, Delivery (90 min) • Self-Evaluation (60 min) • Open Discussion (60 min)

The course includes the following materials:

- OCTAVE Method Training v2.2 Student Notebook,
- OCTAVE Method Training v2.2 Instructor Guidelines,

Note that curriculum for this course does not use the OMIG [OM2]. That is because the OMIG is designed to support the prerequisite to the Train-the-Trainer course, OCTAVE Method Training.

2.2.2 Support OCTAVE Execution

To facilitate transition of the OCTAVE methodology to MTF personnel and encourage its broad acceptance, the DHIAP Team provided ongoing support for execution of OCTAVE risk assessments at all DoD MTFs. The DHIAP Team members—including the DHIAP Trainers, the developers of the OCTAVE Tools (the OCTAVE Automated Tool and Risk Database), and technical information security system experts—provided direct, personal support to MISRT execution of site OCTAVEs.

2.2.2.1 Establish Support Base

Methods/Discussion: The DHIAP Team began this activity by planning how the support base would function, ensuring that the DHIAP Team member who trained a MISRT would be the first line of support for that MISRT. As needed due to the nature or difficulty of the support request, these individuals would involve additional DHIAP Team resources in providing support for the topics indicated in Table 3.

Table 3 - DHIAP Resources for Providing MISRT Support

SUPPORT TOPIC	DHIAP TEAM RESOURCE
OCTAVE Method	ATI DHIAP Trainers, with support as appropriate from TATRC and SEI
Vulnerability Analysis Execution	ATI technical experts
OCTAVE Information Center (OIC) help mechanisms	ATI developers of the OIC
OCTAVE Automated Tool (OAT)	ATI developers of the OAT
Risk Database (RDB)	ATI staff responsible for RDB transition to TATRC, with backup from KRM Associates' RDB developers

To streamline and supplement some activities of the initial personal MISRT support, the DHIAP Team began development of a web-enabled OCTAVE Information Center (OIC) that MISRTs would be able to access through TATRC's Risk Information and Management Resource (RIMR). Use of the OIC would permit MISRTs from around the world to submit questions and receive answers during their normal work hours regardless of their location and time zone, and would facilitate scheduling of any in-person communications that might be preferable or required. Functions planned for the OIC are summarized in Table 4.

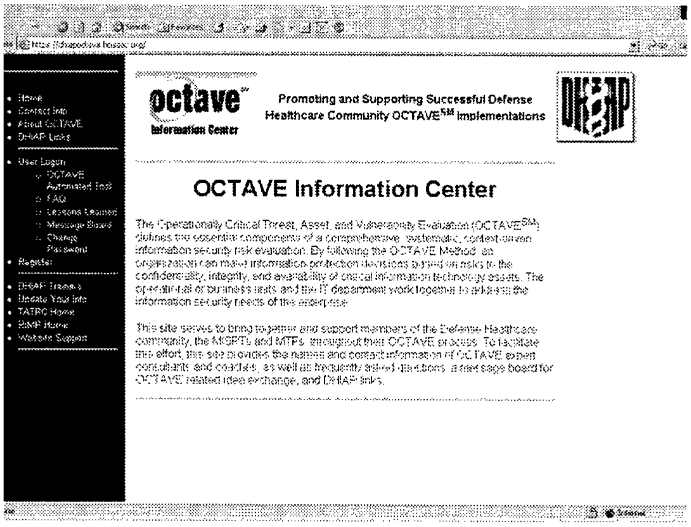
Table 4 - Functions Planned for the OCTAVE Information Center (OIC)

• Home page with general OCTAVE information, including a notional schedule for execution of an OCTAVE risk assessment • Contact Information providing telephone/email contact information for each DHIAP Trainer and other DHIAP staff • Frequently Asked Questions (FAQS) • User Logon and Registration functions	• DHIAP Trainers-Only Area the MTF Support Log) • Links to Information Assurance, Security, and Policy web resources (to RIMR, OCTAVE information sources, the military's HIPAA information, etc.) • An Update Your Information function • Links to the TATRC Home Page, RIMR Home Page, and Website Support

Following the DHIAP Team meeting in early March, the Team began implementing a laboratory to host the OIC and the initial testing of the OCTAVE Tools. (Later on, OAT/RDB testing would migrate to a new server acquired for TATRC's future support of the OCTAVE Tools, and the laboratory server would be dedicated to the OIC.) The initial laboratory environment included two Windows 2000 servers with various hardware and software that made the laboratory environment capable of supporting OIC functionality and similar to what the Team expected OAT Tools testing to require.

Result: The format of the OIC entry-point web page as of the close of Phase III work is depicted in Figure 2. The OIC's major functions are very similar to the functions identified in the original design; a notable addition is the function to permit authorized users (i.e., MISRT members who have completed OCTAVE training) to download a copy of the OCTAVE Automated Tool and then use OIC support request functionality to obtain any support they might need regarding use of the OAT.

Figure 2 - OCTAVE Information Center (OIC) Web Page



Promoting and Supporting Successful Defense Healthcare Community OCTAVE℠ Implementations

OCTAVE Information Center

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE℠) defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets. The operational or business units and the IT department work together to address the information security needs of the enterprise.

This site serves to bring together and support members of the Defense Healthcare community, the MISRTs and MTFs, throughout their OCTAVE process. To facilitate this effort, this site provides the names and contact information of OCTAVE expert consultants and coaches, as well as frequently asked questions, a message board for OCTAVE related idea exchange, and DHIAP links.

OIC functionality included a Trainers-Only area for DHIAP Trainers to use for sharing information with each other. (The function distributes each user question submitted to the OIC to all trainers for their review, and the trainers use it to draft and "discuss" a response—i.e., share drafts among themselves as needed for review/enhancement/correction—before the trainer responsible for providing a response to the user packages the ultimate response and responds directly to the user.) The Team used this function effectively and relatively often throughout the latter portion of Phase III. Ongoing, the DHIAP Team monitored advice given to MISRTs to ensure adequacy, consistency, and accuracy. For queries and/or responses that the Trainers determined would have broad applicability, the DHIAP Team posted items to the OIC's "Frequently Asked Questions" (FAQS) component.

As an extension of OIC development, the DHIAP Team performed a number of activities (summarized in Table 5) to support the OIC and populate it with information that would be of interest to MISRTs and others interested in DHIAP and OCTAVE. They began performing each function as it was implemented in the OIC, and continued the support activities through migration of the OIC to the related ATI-led "OCTAVE Training and Support (OTAS)" contract[2] at the close of Phase III technical work.

Table 5 - Overview of DHIAP Trainer Functions and Activities to Support the OIC

<u>User Registration Support</u> • ***User Registration:*** Adding authorized users (i.e., MISRT members who have attended OCTAVE training) to the OIC's lists of valid users **<u>DHIAP and DHIAP Trainer Support</u>** • ***MTF Support Log:*** Updating the Log with a record of each direct, personal event of providing support to a MISRT; contained within the protected DHIAP Trainers portion of the site, the Log includes details identifying the requestor, date and subject of the request, and a description of how the request was handled and/or resolution to the problem • ***OAT Download Statistics:*** Updating of this table, which is contained within the protected DHIAP Trainers portion of the OIC, is performed automatically by OIC software; updates are posted each time a user downloads a copy of the OAT (Beta version), identifying the user and indicates the date of the download.	**<u>Enhancement of OIC Content for Users</u>** • Publication of FAQs: Adding new entries to the OIC FAQs list as the DHIAP Training leader determines that the subject of a MISRT user's support request or the content of the response is likely to be applicable to a number of other MISRTs • Publication of Lessons Learned: Acquiring and publishing write-ups on the OIC of interesting MISRT approaches to tailoring their site OCTAVEs and the implementation experiences reported by MISRTs that have completed execution of their facility's OCTAVE risk assessment **<u>Technical Support Functions</u>** • Maintaining OIC availability of service • Changing OIC functions and updating OIC content (authorization, change management/configuration control, etc.) • Providing security/access control for protected areas of the OIC (e.g., the Trainers-Only area) • Providing functionality for authorized OIC users to download the OCTAVE Automated Tool (implemented when OAT was made available for Beta testing) and upload OCTAVE results (via OIC to the RDB on RIMR)

Since the DHIAP developers continually coordinated OIC development and enhancement activities with TATRC technical resources to ensure compliance with known RIMR and DoD requirements, the OIC functioned effectively throughout Phase III as an application that was accessed through RIMR but housed at the offices of ATI. At the close of DHIAP Phase III, TATRC authorized continuation of ATI's direct support for the OIC by making it a part of the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

2.2.2.2 Provide Support to MISRTs

Methods/Discussion: Beginning upon completion of the TMA HIPAA Summit 2001 training of the initial group of MISRTs, the DHIAP Team began providing OCTAVE support via direct contact with the DoD OCTAVE users (i.e., the MISRTs trained during OCTAVE deployment and any MTF staff members added to the teams during execution of their sites' OCTAVE risk assessments). By the time the worldwide "wide deployment of OCTAVE" training was initiated, the OIC was fully functional as the entry point for MISRT support requests. Implementation of each new component of the OIC permitted the support to be facilitated more substantially through Internet and e-mail contact. The DHIAP Team provided MISRTs with OIC-based support from the time they were trained on OCTAVE until June 2003 when the support activities were migrated to the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

DHIAP Trainers used e-mail and telephone support, surveys, and other means as appropriate to provide ongoing MISRT support. DHIAP Trainers monitored OIC activity, either responding to an incoming support request or arranging for it to be addressed by the DHIAP subject matter expert responsible for the area of concern. (Assignment of subject matter experts for OCTAVE-related support subjects is summarized above inTable 3 – DHIAP Resources for Providing

MISRT Support.) Responses to MISRT questions were provided in near real time, with speed of the response correlated to the apparent urgency of the situation.

DHIAP Trainers also used various other techniques to maintain lines of communication with MISRTs. A method employed shortly after the HIPAA Summit to open lines of communication between DHIAP Trainers and the trained MISRTs was to create an e-mail account at ATI called "DHIAP Trainers" and use that identity for sending updates and useful news to MISRT members who had attended OCTAVE Training. The DHIAP Trainers e-mail account was configured to automatically forward any MISRT responses to all DHIAP Trainers, facilitating their joint awareness and establishing the opportunity for collaborative action on development of a response.

The first use of a DHIAP Trainers email was a news bulletin to all 156 HIPAA Summit attendees. It announced availability of support through the OCTAVE Information Center, availability of a new CD version of OCTAVE that contained an HTML-browsable copy of the 18-volume OMIG, a reminder that MISRTs should use their DHIAP Trainer as their initial point of contact for support requests, and a request that MISRTs reply to the email with feedback on the status of their facilities' OCTAVEs.

A second DHIAP Trainers e-mail communication was sent to the additional 349 MISRT members trained during OCTAVE Wide Deployment. This e-mail announced availability of the Beta release of the OCTAVE Automated Tool (OAT) for MISRT download, described recent enhancements to the OIC, and announced completion of the OCTAVE Wide Deployment training.

Other forms of support provided to MISRTs during Phase III included telephone conversations, preparation of briefings for senior commanders at MTF sites, and direct/personal e-mail support. All support activity was logged in the OIC's MTF Support Log (which DHIAP Trainers could access through the access-controlled DHIAP Trainers area of the OIC). A copy of MTF Support Log contents as of the end of Phase III technical work is provided in Appendix 2 – MTF Support Log.

As the DHIAP Trainers worked with various MISRTs on startup of their sites' OCTAVEs, they received questions about how to conduct the "shortened" version of the risk assessment, OCTAVE-S. The Trainers helped the MISRTs understand and use various techniques that are part of the "S" version of OCTAVE, and determined that they should personally obtain greater insight into techniques for leading and conducting OCTAVE-S. Using knowledge and materials the DHIAP Training leader had acquired from attending the SEI's OCTAVE-S training in February 2003, Team members guided execution of an OCTAVE-S for ATI and its affiliate, SCRA, between February and April 2003. The experience provided the Team with improved insight on how to respond to MTF MISRTs questions and guide their OCTAVE planning.

Result: Lines of communication between DHIAP Trainers and MISRTs were established upon completion of each round of MISRT training and strengthened through use of e-mails from DHIAP Trainers. The Team received positive response to the DHIAP Trainers email announcements. MISRT members used the DHIAP Trainers who had led their OCTAVE training sessions as their initial point of contact for OCTAVE support; then, as appropriate and necessary, those trainers turned to the support base of DHIAP subject matter experts for knowledge that would let them provide a correct response to each support request.

An example of the effectiveness of the multi-layered DHIAP support infrastructure is a user's request for technical information regarding installation of the Beta version of the OAT on a shared network resource (rather than the on the recommended stand-alone configuration). The DHIAP Trainer who received the request took it to DHIAP's subject matter expert for the OAT and learned that this issue had been encountered and resolved during testing. The Trainer prepared a response to the user's question, reviewed it with the OAT expert to ensure it was accurate, communicated the solution to the MISRT requestor, and recorded the event in the MTF Support Log so that other DHIAP Trainers could benefit from the knowledge.

The DHIAP Team received support requests in numerous ways, ranging from unsolicited emails to the DHIAP Trainers mailbox, to direct personal questions e-mailed or telephoned to individual DHIAP trainers and conversations held in-person in hallways. Since the large number of MISRTs trained during the summer of 2002 were (at best) in the earlier stages of conducting their site OCTAVEs when the time period for Phase III technical work ended, those teams did not have much opportunity to encounter the kinds of difficulties that might make them ask the DHIAP Team for assistance. The OIC's FAQs and other functions were in place to help, and, as noted below, TATRC arranged to extend OIC support beyond the end of DHIAP Phase III technical work by migrating the DHIAP support activities to the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

A large proportion of questions submitted to the OIC asked how to obtain a copy of the OCTAVE Automated Tool (OAT) for use during the site's OCTAVE; some asked about the advisability of using OAT for their sites' OCTAVE since the software was in Beta test. By the end of Phase III, (as depicted in Appendix 3 – OCTAVE-Trained Staff Who Have Enrolled for OIC Access), 59 individuals had obtained a sign-on for access to the OIC and 56 support requests had been addressed and posted to the MTF Support Log. In mid-2003, the DHIAP Team received and acted on support requests from several MISRTs for assistance in planning their sites' OCTAVEs and also for mentoring or directly leading those sites' OCTAVEs.

In addition to providing MISRTs with rapid response to their questions and posting each communication to the OIC's MTF Support Log (and, as appropriate posting appropriate instruction to the OIC FAQs component), the DHIAP Team used knowledge gained from addressing MISRT support requests for other DHIAP purposes. The other purposes included:

- Providing a summary of the support requests (as listed in the OIC's MTF Support Log) to TATRC and DoD quarterly via the DHIAP Phase III Quarterly Report; the reported information included identity of the requestor and site, the nature of the request, and the nature of the response;
- Enhancing OAT functionality; and
- Recommending (through the "Develop Recommendations for Tailoring the OCTAVE Method" task) how DoD should adapt OCTAVE and/or the DHIAP-developed OCTAVE support infrastructure to make them more effective for DoD use in the future.

The Team also used knowledge gained from monitoring and helping with the ATI OCTAVE-S as input for input to the "Develop Recommendations for Tailoring the OCTAVE Method" task.

Success of this task was endorsed when, at the close of DHIAP Phase III, TATRC authorized continuation of ATI support to MISRTs executing OCTAVE risk assessments by making it a core element of the follow-on ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

2.2.2.3 Establish and Implement Feedback Mechanisms

Methods/Discussion: This task was conceived to provide TATRC and MHS with updates on OCTAVE use and risk assessment status throughout MHS. During execution of Phase III, the DHIAP Team developed several ways that MISRTs could provide the feedback.

- One feedback mechanism that the Team began using at the beginning of Phase III took the form of Pre- and Post-Training Surveys. The DHIAP Trainers requested that individuals attending the HIPAA Summit's two-day OCTAVE Training course complete these "before" and "after" surveys. The Team collated and stored results in a central repository of survey data. Then, when analysis of Summit survey results indicated that the Pre-Training Survey provided little useful information, DHIAP leaders decided to drop the Pre-Training Survey from OCTAVE Training, continuing use of the Post-Training Survey for training conducted during OCTAVE Wide Deployment. The Team continued to store survey results in the central repository, allowing for the Post-Training Survey results to grow as a DHIAP OCTAVE Support information resource.
- A feedback mechanism that was considered carefully was to request that MISRTs complete a short customized survey as they reached critical milestones in their OCTAVE progress (e.g. at the completion of Phases 1, 2, and 3). Upon MHS deferral of Phase III OCTAVE Training, the Team abandoned the concept because it was unlikely that very many sites would reach completion of Phases 2 or 3 by the time DHIAP Phase III technical work ended.
- The most effective method for tracking sites' OCTAVE progress and status proved to be the DHIAP Trainers' relationships with MISRTs that they had trained. Through these relationships, sometimes maintained as a byproduct of responding to the MISRTs' support requests, they could learn informally about sites' progress. The Trainers posted the progress information they obtained to the MTF Support Log in the Trainers-Only area of the OIC for future analysis.

Ongoing, the DHIAP Trainers posted results of all status tracking efforts to the MTF Support Log in the Trainers-Only section of the OIC. In this task, the Team utilized the Support Log data, as well as the data contained in the central repository of Post-Training Survey results, to analyze ways to improve the DoD's OCTAVE Training and MISRT Support and provide progress updates for the DHIAP Phase III Quarterly Report.

Result: The DHIAP Team forwarded the knowledge it gained using the various methods of tracking sites' OCTAVE execution status to TATRC and DoD as needed, and documented the findings each quarter in the DHIAP Phase III Quarterly Report. They also retained this information for analysis and reporting in a required project-end task and produced the deliverable, "Recommendations for Tailoring OCTAVE for DoD/MHS use."

2.3 OCTAVE Tools

This task consists of two major subtasks: One designed, developed, and provided a PC-based *OCTAVE Automated Tool (OAT)* to support site execution of OCTAVE risk assessments; the other designed, developed, and installed a *Risk Database (RDB)* for central collection and management of the individual MTFs' OCTAVE/OAT-gathered data.

Figure 3 depicts the series of activities that occur when a user obtains OAT software via download from the OIC (which is accessed through TATRC's RIMR web site) and then, after using the OAT to collect data during a site OCTAVE risk assessment, uploads the OAT-collected data to the RDB. RDB operation is dependent on the OAT, since it is fed solely by information gathered by the OAT during a site's conduct of OCTAVE.

Use of the OCTAVE Tools occurs generally as follows (note that step numbers below equate to the circled numbers in Figure 3):

1. The MTF MISRT downloads OAT from the OIC web site and installs it on the MTF's computer.
2. As each activity of the MTF's OCTAVE risk assessment is performed, the site's MISRT enters OCTAVE-related data into OAT.
3. Upon OCTAVE completion, the MISRT initiates the Transfer Agent function of the OAT and uploads selected OCTAVE data to the OIC's RIMR support.
4. The MTF's OCTAVE data is passed through the OIC web server to the RDB server, where it is held in the Staging Area.
5. The RDB Administrator validates submitted OCTAVE data in the Staging Area.
6. The RDB Administrator moves the validated OCTAVE data to the Risk Database.

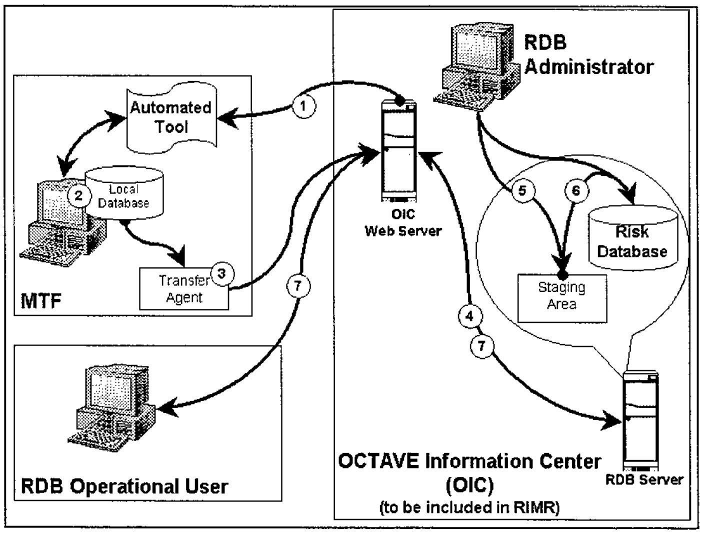


Figure 3 - Interrelationship of OCTAVE Automated Tool / Risk Database

7. An RDB Operational User accesses RDB data via the OIC web server to execute queries against selected groupings of data and either view results (online or in print) or export results to another software product for further analysis.

2.3.1 OCTAVE Automated Tool (OAT)

The OCTAVE Automated Tool effort developed and piloted a PC-based OCTAVE Automated Tool (OAT) to support site execution of the OCTAVE processes. It concluded by turning over a hardened production version of the OAT to TATRC for distribution and use throughout DoD. OAT was designed to guide a site's Medical Information Security Readiness Team (MISRT)—the "Analysis Team" that leads the site's risk analysis effort—through the steps of the OCTAVE process, while also capturing OCTAVE data and generating the interim and final reports associated with the effort. It facilitated the OCTAVE process "scribe" functions, supporting the collection of OCTAVE assessment data, prompting users through the sequence of OCTAVE process steps, and providing links to an electronic version of the OCTAVE Method

Implementation Guide, Version 2.0 (for guidance documentation each OCTAVE process, activity, and step and copies of presentations that could be used in conducting the process).

The OAT Graphical User Interface (GUI) was designed to perform data quality assurance checks during data entry and to retain data in a local OAT database. OAT functionality also included post-OCTAVE support MISRT designation of the data that was to be transferred to the centralized RDB upon completion of the site OCTAVE and an interface to securely transfer the selected data to the RDB. Throughout the OAT development effort, the DHIAP Team coordinated OAT design and activities with work of the RDB (see the "Risk Database (RDB)"section below).

2.3.1.1 Specify Requirements

Methods/Discussion: Based on extensive experience with content and goals of the OCTAVE Method gained while supporting DHIAP Phase II site execution of OCTAVE and also while serving as DHIAP Trainers during the TMA HIPAA Summit 2001, the DHIAP Team began in October 2001 to review and document user requirements for the OAT. The Team identified OAT functional capabilities and technical requirements, and depicted their view of the overall design in a process flow diagram and a series of notional screen formats for the GUI.

Next, the Team examined technical requirements for the OAT development environment and identified equipment that would be required if these tools were selected for use. For OAT application development, they considered fourth generation tools such as Microsoft Access, DemoShield, and ColdFusion, ultimately deciding that Access would be the best fit. (An important factor in selection of Access was that it met the TATRC requirement that OAT software be generally available throughout DoD at no additional cost to the site. The Team determined that Access would typically be included in the Microsoft Office toolset that should be available in all OAT user environments, so there would be no special product acquisition issues, license fees, or learning curve associated with MTF users acquiring and using the OAT.) Using knowledge of the development tools that would be used, the Team reviewed the equipment list that had been prepared earlier in the program and revised it to meet requirements for the Access development environment. They published the revised list in early November 2001.

In mid-November 2001, the DHIAP Team PI and software developers met with TATRC to review and refine user requirements for the OAT, describing requirements for OAT functional and technical capabilities at both the system and software levels.[3] The Team used the process flow and notional screen format documentation to describe the context for integrating OAT with a site's execution of the OCTAVE process, pointing out how the OAT general design met the following fundamental requirement:

> The scribe/facilitator will use the Tool to complete an OCTAVE. It will capture all OCTAVE data that the scribe would retain and carry forward to a future process (i.e., that information upon which group consensus has been obtained).

Comments resulting from the November OAT review were incorporated into the OAT requirements documentation and equipment requirements. Definition of detailed requirements for the OAT was completed in November 2001 and published in the DHIAP Phase III Technical

[3] The "system" is the complete OCTAVE Automated Tool package. The "software" is the primary component of the system but refers specifically to the automation of the OCTAVE process.

Development Plan [TD3]. (Note that final requirements for the RDB were also confirmed and approved at this time so that the OAT and RDB designs would be consistent and complementary.)

Result: The TATRC-approved System Requirements and Software Requirements for the OAT were published in [ANN] Appendix 5.3. TATRC and the DHIAP Team agreed that the following Common Off-The-Shelf (COTS) development tools would be used in the core OAT development effort: Microsoft Access 2000 and its built-in Visual Basic 6.3. With all system and software requirements agreed upon, formally documented, and well understood by TATRC and the developers, the OAT requirements were ready for use in the next task, development of the system and software architecture. (Note that final requirements for the RDB were also confirmed and approved at this time so that the OAT and RDB designs would be consistent and complementary.)

2.3.1.2 Develop System and Software Architectural Design

Methods/Discussion: Using as guidelines the requirements specifications from the previous task and technical characteristics of the selected COTS development tools, the DHIAP Team developed a top-level design for the OAT technical components. Design documentation included:

- GUI design with draft screen formats to be used in the application, along with descriptors indicating special processing and/or editing requirements for the data entry fields;
- Design of the OAT's local database (e.g., field length, alpha vs. numeric representation, range of acceptable values, etc.);
- Design of interfaces to external software and between the OAT's software components;
- Design for the upload capability to interface to the central RDB;
- Preliminary drafts of user documentation;
- Design for integration of OAT with the OCTAVE Method, Version 2.0; and
- Preliminary test procedures.

The DHIAP Team met in mid-January 2002 to develop the preliminary system architecture for the OCTAVE Tools—both the OAT and the RDB. To effectively describe the systems design, they drafted documentation that depicted the multi-step operational cycle of using the Tools from the viewpoint of the user (see Figure 3) and prepared additional documentation of the process steps, major processes and operational components of each step, equipment requirements at each step, and lists of issues or unknowns that related to each step. Following the meeting, the Team sent the architecture materials to TATRC, discussed the materials with TATRC, revised the documentation to incorporate TATRC's input, and published a draft OCTAVE Tools Architecture.

Based on experience gained from working with the OCTAVE Tools Architecture, the Team members met again in early March 2002 to review and update the documentation, the development plan, and test plans. Included in the group's discussion of plans for testing the OCTAVE Tools was a discussion of TATRC's interest in having a small, knowledgeable group of individuals evaluate and test the OAT at an earlier stage than had been called for in Phase III schedules. The Team updated the draft test plan and schedule to include a cycle for TATRC testing of the Alpha version of the OAT and, at TATRC's discretion, testing by an OCTAVE-experienced MTF (i.e., an MTF that had been trained on OCTAVE during Phase II and completed a site OCTAVE). The Team conducted a design review with TATRC, and incorporated TATRC input into the design.

Next, the Team performed an in-depth analysis of OAT and RDB database schemas to determine any changes that would be required for OAT to share site-collected data with the RDB. In a discussion of the overall schedule for development and release of succeeding versions of the OCTAVE Tools, the Team adjusted schedules based on the revised testing approach and recent experience gained from working with the OAT and RDB development tools. The Team confirmed decisions made about database schemas for the OAT and RDB by publishing a document that compared the schemas to be used in each tool.

Throughout the design process, the Team coordinated OAT design decisions with the designers/developers of the RDB and other relevant stakeholders (e.g., SEI's OCTAVE Method developers) to ensure functional compatibility across all OCTAVE-related products.

Result: The DHIAP Team used the System and Software Architectural Design documentation and the schedule that had been revised for rapid development/early user testing as guidelines for planning and executing the next task, Software Coding, Testing, and Integration.

2.3.1.3 Perform Software Coding, Testing, and Integration

Methods/Discussion: The Team began this work by acquiring and installing the selected COTS development tools. They coded and integrated the software components according to the design developed in the preceding task. To reduce development time, they utilized capabilities of the development support tools to the maximum extent possible, producing a prototype OAT that consisted of the GUI and the local database.

The OAT prototype provided screens and functionality to enter facility demographic data, guide the user through OCTAVE Processes 1-8, track progress toward completion of the OCTAVE, and display/print documents such as numerous interim reports, Asset Profile Workbooks, and the Final Report. In February 2002, the Team sent a very early OAT prototype to TATRC for preliminary review.

Selected DHIAP Team members reviewed, tested, and evaluated OAT prototype software for usability and processing accuracy. The developer enhanced individual software units and components of the OAT software to address issues identified during the internal testing, and produced an Alpha version of OAT in March 2002. The developer demonstrated the Alpha OAT to TATRC and other DHIAP Team members at the March 2002 Team meeting. The Team performed some initial in-house OAT usability testing later in March 2002, and then conducted a more formal test of the Alpha version in early April 2002. Throughout this activity, the Team developed and enhanced the OAT's user documentation. (While most user documentation was included within the OAT itself, some was also created for use as external paper or electronic support.)

Also during this period, the Team developed support materials for Usability Tests to be conducted by other DHIAP-related groups. Those materials included Usability Test Instructions and Feedback Forms, as well as an OAT Test CD installation package that contained a self-extracting OAT application (Alpha version), an electronic copy of the OCTAVE Method Implementation Guide (OMIG) Version 2.0, and the Usability Test Instructions.

In mid-April 2002, the developers delivered copies of the OAT Test CDs to TATRC and to DHIAP Team members at SEI and BWXT Y-12 LLC. For the TATRC and SEI deliveries, the developer demonstrated use of the OAT and led discussion of the goals of the test and the preferred format and timing for feedback. SEI representatives provided their feedback in mid-May, and usability testing feedback from the other test groups—BWXT Y-12 LLC, TATRC, Georgetown University, and the Naval Medical Information Management Center (NMIMC)—was provided by June 2002. (Georgetown and NMIMC were given copies of OAT by TATRC in return for a commitment to provide feedback to the developers.)

Preliminary to addressing any feedback from the OAT Alpha version tests, the DHIAP Team established a configuration control process that included reviewing feedback from internal OAT users and the remote testers, analyzing the impact of changes to both the OAT and the RDB, and determining the sequence of execution for the approved changes. To support the process, the Team implemented a method that is similar to the DHIAP management's Action Items List to record, prioritize, and track requests for OAT refinements.

Feedback from the DHIAP Team's Alpha testing varied in its level of detail from general impressions to specific issues. DHIAP leaders determined which issues were essential to fix, and the developers resolved them through updating the software or changing the OAT's online documentation as appropriate. The two most significant OAT refinements arising from Alpha testing were to implement threat profiles in the form of threat trees as utilized and depicted in the OMIG and to provide a more usable format for the Survey Summary Report. Throughout the OAT testing and enhancement process, the OAT developers maintained communication (primarily through use of the database schema documentation) with the RDB developers to ensure that OAT database changes would be appropriately reflected in the RDB database and functionality.

Result: Results of each testing cycle were used to enhance OAT functionality or revise screen formats and OAT-based "help" documentation to be more usable. Completion of these efforts produced a hardened Alpha version of the OAT.

2.3.1.4 Perform Software Qualification Testing

Methods/Discussion: To ensure that OAT capabilities conformed to the system and software requirements developed earlier in the project, that external and internal operations were consistent with system requirements, and that user documentation was up-to-date, the DHIAP Team conducted functionality and usability testing of the OAT in the DHIAP laboratory in August 2002. In conducting these tests, the Team followed the sequence of activities and used data provided in the OMIG's example case study.[4] They documented all issues and concerns arising from the test. DHIAP Team leaders again used the configuration control process to determine which issues were essential for accurate processing and/or usability, and the developer changed the software and/or the OAT's online documentation as appropriate for addressing the issues.

Modifications made to the OAT at this point included some restructuring of the underlying database schema and further development of the Visual Basic code (and associated documentation and error handling) supporting much of the OAT's automation. The Team

[4] "OMIG Volume 17: Appendix C—Complete Example Results" in [OM2] provides an excellent recap of the case study data, although some information needed for testing can be found only in the workshop manuals.

enhanced nearly every OAT form and report in some way during this effort. Some of the more significant enhancements in the resulting Beta version of the OAT included: adding contextual help tips, improving processing of user survey questions so only the questions applicable to the workshop were displayed, improving formatting of the survey summary report, adding a step to obtain user confirmation before executing user commands to delete data (and making this function appear consistent across all forms), and removing record navigation buttons from places where they were not applicable. The most significant change reflected in the Beta version was to allow the user to create threat and risk profiles in an automated, graphical manner that was virtually identical to the threat trees presented in the OMIG.

The Team's enhancements to create the OAT Beta version also addressed some functions to support the OAT's interaction with the OIC and RIMR. They included completing development of an OAT download and installation package (created with the COTS product, DemoShield) that enabled users to obtain the OAT directly from the OIC, adding links to a "Getting Started" guide, and preparing the data file that would be used for OIC upload (i.e., to upload selected data from the site's OCTAVE to the RDB).

Result: Through this series of usability and functionality tests, the OAT was enhanced to be both usable and dependable for supporting the execution of site OCTAVE risk assessments. With completion of this task, in-house testing of the OAT Beta version by ATI, SEI, and TATRC was completed, refinements determined to be necessary were made to the OAT, the package to support a site's OAT download from the OIC was tested and proven, web pages to guide Beta testers in downloading OAT were posted to the OIC. All functionality needed for trained MISRTs to test the OAT Beta version while they conducted their sites' OCTAVEs was in place and operational.

2.3.1.5 Perform System Integration and Qualification Testing

Methods/Discussion: Original DHIAP plans for this task had called for the DHIAP Team to test the usability of the OAT Beta version by working directly with the experienced MISRT at a trial site selected by TATRC. However, based on the large number of requests that DHIAP Trainers received during the rollout of OCTAVE training to MISRTs, TATRC observed that it would be helpful to DHIAP and to MHS HIPAA readiness overall if the OAT could be made available for field use earlier than planned. Therefore, in September 2002, the DHIAP Team announced to MISRTs that the Beta version of OAT was available via download from the OIC for their use. (The announcement included a warning that MISRTs might encounter difficulties in using the OAT because it was Beta software.) A number of MISRTs responded that they would like to use the OAT, acknowledged that the software was a Beta release, and agreed to provide feedback following completion of their OAT use (i.e., "test"). The MISRTs then proceeded to follow OIC instructions for downloading and using the software.

Result: As shown in Table 6, ten sites downloaded OAT for Beta testing and use in their site OCTAVEs.

Table 6 - OAT Beta Test Sites

SITE / FACILITY NAME	DOWNLOAD DATE	SITE / FACILITY NAME	DOWNLOAD DATE
ISIS	13-Sep-02	Tripler Army Medical Center	9-Oct-02
140th. Medical Squadron	13-Sep-02	121 General Hospital	15-Oct-02
USCG MLCLANT	16-Sep-02	78 Medical Group	18-Oct-02
7 MDG Dyess AFB	17-Sep-02	BMC Sasebo	22-Oct-02

SITE / FACILITY NAME	DOWNLOAD DATE	SITE / FACILITY NAME	DOWNLOAD DATE
BMC Iwakuni	17-Sep-02	18 MDG Kadena AB	22-Oct-02
140 MDS	20-Sep-02	3rd Medical Group	23-Oct-02
National Naval Dental Center	23-Sep-02	374th Medical Group	28-Oct-02
USNH-Guam	23-Sep-02	NH GTMO	29-Oct-02
USNH Okinawa	25-Sep-02	Naval Hospital Bremerton	29 Oct 02
TRICARE Mid-Atlantic	3-Oct-02	3rd Medical Group	31-Oct-02

The DHIAP Team gathered feedback on OAT usability and technical features throughout qualification testing, via questions submitted through the OIC and through various forms of direct MISRT contact. While the OIC input from OAT users in the field consisted mostly of requests for access to the OAT download function; the MISRTs' comments regarding their OAT use were positive and no processing errors were reported from the field.

2.3.1.6 Refine Tool and Develop Installation Package

Methods/Discussion: When the schedule for field use of the OAT by MTFs was accelerated to allow recently trained MISRTs to use the Beta version of OAT as they executed site OCTAVEs, the DHIAP Team had to begin work earlier than planned on the portion of this task that supported upload of OCTAVE results to the central RDB resource. As OAT development reached each new level of stability during Alpha and Beta version development, the DHIAP Team addressed development and testing of the related software that would accomplish downloading the OAT from the OIC and transferring data from a site's OAT to the RDB. The majority of this development and its initial testing occurred during July-August 2002. Based on the plan to release the Beta version to MTFs, additional testing of the transfer functions was planned and conducted in DHIAP Team meetings beginning in late August 2002.

Result: The Team produced an OAT installation package that was a self-contained application. Through use of the COTS product, DemoShield, and its executable "wizard" that incorporates the COTS InstallShield, the package permitted users to download a set of instructions and the OAT from the OIC and then install it. Support for the post-OCTAVE data transfer from the OAT to the RDB was developed in a modular manner, with each component finalized at a time that was appropriate based on the RDB's planned development cycle.[5]

2.3.1.7 Provide Support for the Automated Tool

Methods/Discussion: As was true for the preceding two tasks, changes to the schedule for MTF field use of the OAT led to beginning work on this task earlier than originally planned. The first line of support for MTF users of the OAT Beta version was the OIC. Because MTF use of the OAT was just beginning as of the end of Phase III, most OIC requests related to guidance on downloading the OAT. In providing OAT support, where the OAT developers determined that a problem should be fixed through operational procedure, the Team responded to the requestor as appropriate and also captured the information for potential inclusion in the OIC's FAQs. When a problem related to software/hardware issues, the most appropriate DHIAP resource (whether the OAT developer or the OIC staff) worked with the MISRT to accurately define the problem and to develop and implement the fix.

[5] Phase III schedules called for most of the RDB development to occur following OAT development and testing feedback, minimizing the amount of rework necessary to ensure that the RDB appropriately supported all OAT functionality.

Result: The OIC Support Log recap of requests for OIC assistance (see Appendix 2 – MTF Support Log) includes the requests relating to MTF use of the OAT Beta version. The DHIAP Team provided MISRTs with OIC-based support for the OAT from the time they were trained on OCTAVE until June 2003 when support activities migrated to the related ATI-led program, "OCTAVE Training and Support (OTAS)."[2]

2.3.1.8 New Tasks Defined for the Phase III No-cost Extension

Methods/Discussion: In the Phase III tasks described above, the OAT was developed, tested by ATI and SEI, and provided to TATRC and MHS for review, testing, and comment. Feedback from the various levels of testing and some limited public exposure was used to enhance the OAT and produce a Beta version. The Beta release was tested by ATI, provided to SEI for additional testing, and offered to MISRTs that had attended OCTAVE MISRT training for their use in the field while conducting their sites' OCTAVEs. As an extension of the OIC support function, OAT developers supported the military "field" users of the OAT through the scheduled end of Phase III and collected/documented suggestions for Tool enhancement.

For the no-cost extension timeframe (February-August 2003), ATI proposed (and TATRC agreed to) a continuation of OAT- support and enhancement. Specific tasks of the extended effort were:

- Select Enhancements from Support Feedback;
- Code Enhancements;
- Test Production and Release to Field for Acceptance; and
- Support Production Version of OCTAVE Automated Tool.

Since the OAT would be used by a number of military field users as the repository for data collected during execution of their OCTAVEs, this task would provide the basis for (1) supporting an extended Beta test of the OAT if deemed necessary, (2) identifying essential OAT enhancements based on feedback provided during field use, (3) updating the Beta version to include the selected enhancements as part of testing; and (3) releasing the production version.

The DHIAP Team supported the OAT Beta version during an extended period of testing, gathering input on enhancements that might be desirable or were proving to be necessary. The most significant enhancement selected from the support feedback was to provide more flexible support for entering and managing data associated with OCTAVE's Process 5-6 technical vulnerability assessments. Other enhancements included improvements to the capability for tracking completion of each OCTAVE process, the ability to update and save threat and risk profiles, and some changes to the function for post-OCTAVE data upload to the RDB. The Team updated the Beta version of OAT to include the selected enhancements, tested the software, and packaged the production version of OAT as "DoD-MTF 1.0.1."

Beginning in May 2003, the Team conducted security testing of the OAT and began drafting the System Security Authorization Agreement (SSAA) documentation that would be evaluated during OAT security testing. To facilitate preparing OAT and RDB for certification and accreditation by the DoD, the DHIAP Team enhanced the OAT and RDB test plans to include additional testing procedures and additional pre-C&A documentation. The test plan and documentation updates reflected requirements established by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Sections of the DITSCAP System

Security Authorization Agreement (SSAA) that the Team determined were applicable to the OAT, RDB, and TATRC were completed to provide the information that would be required if TATRC proceeds with submitting OAT and RDB for a full certification and accreditation process.

To align the DHIAP Team's OAT and RDB security testing with DITSCAP requirements, the DHIAP Security Test Team used the Minimal Security Checklist as described in the DITSCAP Application Manual (DoD 8510-1M) [DTS] for a major portion of the OAT and RDB security test plans. The DHIAP Security Test Team met with the OAT and RDB software developers to ensure that certain security requirements described in this checklist were included as part of the software development life cycle, and also to define functionality, security requirements and features, and software criticality.

During the course of security testing for the OAT, the Team identified and corrected over 100 security issues. The majority of these issues stemmed from the fact the Visual Basic modules supporting the OAT functionality lacked the "Option Explicit" statement. (While an "Option Explicit" statement is not necessary for OAT operation, it is valuable from a security point of view because it prevents the code from allowing undeclared variables.) Although no security issues were identified that would impact DoD's use of the OAT production version DoD-MTF 1.0.0, the Team revised the OAT code to include the "Option Explicit" statement in all modules and ensured that no variables were undeclared. In a complementary activity, the Team ensured that no declared variables in the OAT code were unused.

The DHIAP Team arranged for the Naval Hospital Charleston (NHC) to test the OAT production version DoD-MTF 1.0.1 during the site's May-August 2003 execution of the OCTAVE Method. This allowed the Team to gain firsthand knowledge of OAT operation as an extension of normal DHIAP activity to provide support to site Analysis Teams during OCTAVE execution (see "Since the DHIAP developers continually coordinated OIC development and enhancement activities with TATRC technical resources to ensure compliance with known RIMR and DoD requirements, the OIC functioned effectively throughout Phase III as an application that was accessed through RIMR but housed at the offices of ATI. At the close of DHIAP Phase III, TATRC authorized continuation of ATI's direct support for the OIC by making it a part of the related ATI-led contract, "OCTAVE Training and Support (OTAS)."2

Provide Support to MISRTs" above). Responsibility for NHC OAT support was transferred to the related ATI-led program, "OCTAVE Training and Support (OTAS),"[2] in June 2003 when all other OCTAVE support activities migrated to that effort.

Result: By mid-March 2003, the initial OAT production version DoD-MTF 1.0.1 had been coded and tested, and the software was ready for packaging and distribution. By mid-April 2003, ATI and TATRC had each successfully tested downloading the production version of OAT from the OIC and installing it on a local computer. By the end of May 2003, the DHIAP Team had completed OAT security testing, made appropriate changes to the software, and completed preparation of the preliminary SSAA documentation that TATRC would later use when having a DoD Information Technology Security Certification and Accreditation (DITSCAP) conducted for the OAT.

2.3.2 Risk Database (RDB)

The Risk Database effort developed, piloted, and turned over to TATRC for ongoing operation the Risk Database (RDB)—a repository for OCTAVE data collected during site information assurance risk assessments. RDB design called for data to be transferred from OAT to the RDB via an interface implemented as a component of the OCTAVE Information Center (OIC). (As permitted by DoD security, policy, and technical requirements, access to the RDB resource was also to be made available through TATRC's Risk Information Management Resource (RIMR)).

The RDB's purpose was defined to be support for data analysis and consolidation activities necessary for DoD to identify and investigate system-wide information assurance risks. Because of OAT and RDB interdependency, the DHIAP Team coordinated RDB design and development with OAT design and development activities throughout Phase III. To use resources efficiently and minimize the need for rework on the RDB, DHIAP leaders scheduled design and updating of the RDB database architecture as needed throughout OAT development and testing, but deferred most RDB development until OAT was relatively stable and likely cause little reason for modifying RDB software.

2.3.2.1 Specify System and RDB Capability Requirements

Methods/Discussion: Similar to activities described for the OAT, initial input on RDB requirements was obtained during October and November 2001 meetings with TATRC. Based on user requirements that TATRC representatives had gathered in their work with the DoD-MHS user community, the requirements outlined functional, technical, and operational capabilities that were needed in a central repository of sites' OCTAVE-derived information. Because input data to the RDB would be output from the OAT, DHIAP leaders ensured that definition of the RDB's functional and technical requirements were closely coordinated with the OAT requirements definition effort.

Further development of RDB functional requirements by the DHIAP Team included conducting an analysis to determine how to capture and maintain independence of multiple instantiations of OCTAVE site data, identifying interface and interaction requirements of both operational users and the RDB support staff (i.e., the database administrators), determining reports that the RDB should be capable of generating, and identifying user interface specifications for extracting information from the RDB.

Development of RDB technical requirements was based on the functional requirements. The Team analyzed the functional requirements and constraints provided by TATRC in relation to RIMR's operating environment. They evaluated capabilities of COTS tools for meeting RDB technical and operational requirements for: data storage and retrieval, interface with other systems and databases (e.g., with the OAT), security, and report generation. Requirements identified in the RDB documentation were based on the following fundamental requirement:

> The RDB will allow users (as authorized by the DoD) to analyze data collected from sites' execution of OCTAVEs.

The DHIAP Team documented RDB system requirements as sets of functional capabilities, technical requirements, and operational requirements. They also prepared an outline of the user documentation (including installation and operation guidance, etc.) to be developed for the RDB.

In October and November 2001, the DHIAP Team conducted formal reviews of RDB requirements with TATRC and the rest of the DHIAP Team, obtained feedback on the recommendations, assumptions, and design decisions, and incorporated the feedback into the documentation as appropriate. In the mid-November meeting with TATRC, the Team also confirmed appropriate portions of RDB requirements with RIMR support staff. (Note that final requirements for the OAT were also confirmed and approved at this time so that the OAT and RDB designs would be consistent and complementary.)

Result: The approved RDB Assumptions, Functional Capabilities, Technical Capabilities, and Operational Capabilities (plus a final section on User Documentation), were published in [ANN] Appendix 5.4. With requirements for the RDB agreed upon, formally documented, and well understood by the developers, the DHIAP Team used the OAT and RDB requirements as their guide for the next task, selection of the development environment. (Note that final requirements for the OAT were also confirmed and approved at this time so that the OAT and RDB designs would be consistent and complementary.)

2.3.2.2 Select Development Environment

Methods/Discussion: To facilitate integrating the RDB with existing DoD systems and to minimize training and maintenance burdens that might be placed on DoD support personnel, TATRC directed the DHIAP Team to use Oracle8i (and its associated tools) and ColdFusion as the database development and support software. Additional TATRC guidance indicated that the RDB was to be developed so that it would be maintainable by a database administrator experienced in Oracle. To meet these requirements, the Team confirmed that they would use tools such as Cold Fusion, Visual Studio, etc. to support the implementation of the RDB.

Result: TATRC and the DHIAP Team agreed that the following Common Off-The-Shelf (COTS) development tools would be used in the effort: Oracle8i (later upgraded to Oracle9i to remain consistent with RIMR), ColdFusion Server 5, and UltraDev 4 Studio.

2.3.2.3 Develop Architectural Design

Methods/Discussion: Using the requirements specifications from the previous tasks (see "Specify System and RDB Capability Requirements" and "Select Development Environment" above) and the technical criteria of the selected COTS development tools as a guide, the Team developed a coordinated top-level design for the technical components of the RDB. Activities of this task were described in the concurrently executed OAT task described above in "Develop System and Software Architectural Design," as follows:

> "The DHIAP Team met in mid-January 2002 to develop the preliminary system architecture for the OCTAVE Tools—both the OAT and the RDB. To effectively describe the systems design, they drafted documentation that depicted the multi-step operational cycle of using the Tools from the viewpoint of the user (see Figure 3) and prepared additional documentation of the process steps, major processes and operational components of each step, equipment requirements at each step, and lists of issues or unknowns that related to each step. Following the meeting, the Team sent the architecture materials to TATRC, discussed the materials with TATRC, revised the documentation to incorporate TATRC's input, and published a draft OCTAVE Tools Architecture."

Result: The DHIAP Team used the System and Software Architectural Design as their guide for the next tasks.

2.3.2.4 Develop Test Plan

Methods/Discussion: As reported previously for OAT in "Develop System and Software Architectural Design:"

> "Based on experience gained from working with the OCTAVE Tools Architecture, the Team members met again in early March 2002 to review and update the documentation, the development plan, and test plans."

Result: The DHIAP Team test plan development activities focused on defining an approach to ensure that the RDB accurately acquires an OAT data file, accurately converts it to Oracle format, properly stores the data, and properly represents sites' OAT data in the displays and reports generated by the system. The plan includes validating the accuracy of reports and security of the OAT-RDB data transfer.

2.3.2.5 Design and Create the Database Structure

Methods/Discussion: As reported for OAT in Develop System and Software Architectural Design above:

> "Next, the Team performed an in-depth analysis of OAT and RDB database schemas to determine any changes that would be required for OAT to share site-collected data with the RDB. In a discussion of the overall schedule for development and release of succeeding versions of the OCTAVE Tools, the Team adjusted schedules based on the revised testing approach and recent experience gained from working with the OAT and RDB development tools. The Team confirmed decisions made about database schemas for the OAT and RDB by publishing a document that compared the schemas to be used in each tool.
>
> "Throughout the design process, the Team coordinated OAT design decisions with the designers/developers of the RDB and other relevant stakeholders (e.g., SEI's OCTAVE Method developers) to ensure functional compatibility across all OCTAVE-related products."

Based on knowledge gained from dealing with OCTAVE data collected by many diverse types of organizations, the SEI was able to identify some limitations to the initial RDB database design that might have hampered RDB capabilities for reporting across multiple OCTAVE executions. These DHIAP Team members provided the developer with a high-level mapping of the relationships of the data elements collected in OCTAVEs (including data elements added for various tailored versions of OCTAVE that they had developed) to aid in enhancing design of the RDB. This information was used in RDB design to construct an environment that should not be limited by either the current OAT data schema or by the current version of OCTAVE.

Result: The RDB database schema was updated a number of times since its initial development, each update made in association with changes made to the OAT database schema. (Note that the OAT changes were necessitated by software updates that enhanced the OAT through the series of its interim/final Alpha and Beta versions.)

2.3.2.6 Design and Develop the RDB User Front-End (Web Interface)

Methods/Discussion: The DHIAP Team installed and configured the ColdFusion Server, ColdFusion 5, UltraDev 4 Studio, Netscape's web server, and Oracle8i to establish the RDB design/development environment. The RDB users' browser-based interfaces were developed and then demonstrated at the March 2003 DHIAP Team meeting. Based on decisions made at that meeting, the Team defined some updates to RDB data schemas/data relationships and to the OCTAVE Tools Architecture and enabled development of appropriate updates to the RDB user interfaces.

In March 2003 the Team began a pilot test of the RDB development server, including: installing web server software, generating SSL certificates, and ensuring that Perl scripts used on the site were functional in a Windows environment. To support that testing, the Team initiated development activities for the OCTAVE Information Center (OIC), which would later be used to support MISRTs, building the initial OIC website capability for testing the uploading of site OCTAVE data from the OAT to the RDB.

Later RDB development activities included such important functions as:

- System Security at two levels—for System Administrators and for Researchers;
- Reporting functions, including the ability to generate reports on Vulnerabilities, Assets, Threats, Action Items, Protection Strategies, and Demographic Data;
- Ad hoc report generation;
- Capabilities to print RDB output and/or to export it to Word and Excel; and
- Capabilities for sorting and selecting RDB data based on MTF, facility, OCTAVE, TRICARE Region, and Branch of Service.

Result: Initial versions of the RDB user GUI and initial RDB Administrator GUI were developed to support testing administrator and user access to the RDB.

2.3.2.7 Develop Report Functions

Methods/Discussion: As a result of decisions made in the March 2003 Team meeting, the DHIAP Team was able to begin designing and developing the standard reports to be generated by the RDB. Reporting functions included the ability to generate reports on Assets, Threats, Vulnerabilities, Action Items, Protection Strategies, and Demographic Data. As appropriate, many RDB reports utilized the RDB capability for sorting and selecting data based on MTF, facility, OCTAVE, TRICARE region, and branch of service. In addition, the Team developed an ad hoc report generation capability, as well as a function to print any Web output and to export it to Microsoft Word and Excel.

Dynamic menus were developed throughout the system support the RDB reporting functions. The menus, indicating where the user is positioned in the reporting and/or update process, could be minimized once a report had been run to enable capturing screen shots of the information. Other reporting enhancements developed at the time included the ability to click on a portion of a graph (e.g., a pie chart) to display the data behind the graph.

Result: Standard reports were defined and developed. Testing of the reports utilized both generalized and extensively customized datasets. The data successfully generated reports that the Team and TATRC had determined were of interest to the groups that would monitor the security assessment processes within the DoD medical community. In addition to providing standard RDB reports, the reporting function permitted the RDB Administrator to create ad hoc reports to address non-standard user requests for information.

2.3.2.8 Test, Demonstrate, and Enhance the Risk Database

Methods/Discussion: Initial RDB testing was conducted in the KRM developer's laboratory using data created to simulate approximately twenty completed OCTAVEs. The developer's testing of RDB usability features addressed:

- Dynamic menus indicating where the user is positioned in the reporting and/or update processes, and ensuring the menus could be minimized once a report had been run (to enable capturing screen shots of the information);

- Data handling features for the RDB output display supporting clicking on a portion of a graph to initiate a display of the data it represents; and
- Various reporting features and enhancements.

To complete the RDB testing and begin preparation for the upcoming RDB implementation at TATRC, the Team configured an RDB server in ATI's DHIAP Laboratory to match the developer's server environment. The Team loaded copies of all RDB-related software onto the ATI-RDB server, and then extensively tested all aspects of the RDB server and application for functionality, organization, and meaningful output.

The RDB testing activities conducted between March 2003 and May 2003 used data provided by the OAT developers. It included extensive testing of processes for Importing, Reviewing, and Releasing OAT data, as well as testing of the RDB's Reporting and Graphing functions. Errors that were found in the process were resolved by modifying the SQL or application code as needed. Discovery of some anomalies in the demonstration data provided by the OAT developers allowed the RDB developers to enhance the RDB's ability to handle user errors.

At a point when testing had proven the RDB to be relatively dependable, the DHIAP Team in the ATI DHIAP laboratory migrated the RDB Server from use of Windows IIS (installed to conform to the developer's technical environment) to the TATRC standard, Iplanet. When that was working, the Team installed a copy of the OIC on the RDB computer and tested/verified the OCTAVE Tools capability to download OAT software from the OIC and to upload OAT data to the OIC/RDB.

The DHIAP Team demonstrated the OAT upload of data to the RDB and the functionality of the RDB for TATRC in a meeting in early May 2003. In that meeting, TATRC suggested minor modifications to the OAT upload process that would clarify for the OAT user what was happening during the operation. The Team implemented the modifications, and also implemented a TATRC website as the default URL for OAT data uploads. Based on the May testing, the DHIAP Team determined that they could improve the RDB's ability to read data from the OAT database by implementing a new table indicating the OCTAVE data fields that a site had elected not to transmit to the RDB (i.e., the data that the site chose to omit from the upload file). As a result, the developers added another table to the OAT and updated the RDB software accordingly.

The RDB development plan called for final RDB testing to utilize data created when MISRTs in the field used the Beta version OAT to conduct their site OCTAVEs. Since no MISRTs had uploaded OAT data to the RDB as of the end of Phase III technical work in August 2003, it was not possible to perform this testing in DHIAP. Therefore, responsibility for this activity was transferred in August 2003 to the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

As part of the no-cost extension to Phase III efforts, ATI proposed and TATRC approved expanding this task's testing to include security testing and preparing appropriate documentation to a standard, and in a format, that would be expected for submission to a DAA for a C&A designation of Interim Authority to Operate (IATO). Individuals within the program who were independent of the RDB development effort would perform the required testing and documentation. RDB security testing would be performed independently of OAT security testing, so that the RDB could be released as a stand-alone tool for DoD use. Following that, the Team would conduct final security testing for the OAT and RDB together as a system.

As described above in "New Tasks Defined for the Phase III No-cost Extension" for OAT Security Testing:

> "To facilitate preparing OAT and RDB for certification and accreditation by the DoD, the DHIAP Team enhanced the OAT and RDB test plans to include additional testing procedures and additional pre-C&A documentation. The test plan and documentation updates reflected requirements established by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Sections of the DITSCAP System Security Authorization Agreement (SSAA) that the Team determined were applicable to the OAT, RDB, and TATRC were completed to provide the information that would be required if TATRC proceeds with submitting OAT and RDB for a full certification and accreditation process.
>
> "To align the DHIAP Team's OAT and RDB security testing with DITSCAP requirements, the DHIAP Security Test Team used the Minimal Security Checklist as described in the DITSCAP Application Manual (DoD 8510-1M) [DTS] for a major portion of the OAT and RDB security test plans. The DHIAP Security Test Team met with the OAT and RDB software developers to ensure that certain security requirements described in this checklist were included as part of the software development life cycle, and also to define functionality, security requirements and features, and software criticality."

Result: By mid-July 2003, the DHIAP Team had completed OAT security testing, made appropriate changes to the software, and completed preparation of preliminary SSAA documentation that TATRC would later use when having a DoD Information Technology Security Certification and Accreditation (DITSCAP) conducted for the OAT.

2.3.2.9 Develop RDB Management Guidelines Document

Methods/Discussion: Throughout the RDB testing and activities to implement the RDB Server in the ATI DHIAP laboratory, the DHIAP Team drafted and updated elements of the manuals on RDB Management. The Team published the notes in the form of a draft manual in late June 2003 and then used the draft during the mid-July implementation of the RDB Server at TATRC (see "Transfer RDB to RIMR" below). During the installation at TATRC, the Team updated the document as appropriate based on knowledge gained and questions that were asked by TATRC staff.

Result: The DHIAP Team published "Risk Database Administrator's Operation and Maintenance Manual" [RDA] in July 2003. It contains the following types of technical information related to operating and supporting the DHIAP Risk Database:

- RDB Server Hardware Requirements;
- RDB Server Software Requirements (including a description of the RDB's use of the following: RDB Server Authentication Flow and Data Flow, Oracle 9i Database Server, Iplanet Web Server and Directory Server, ColdFusion Server V5, Antivirus Software, and Microsoft Office Professional);
- OCTAVE;
- OCTAVE Information Center (OIC);
- OCTAVE Automated Tool (OAT);
- RDB Server Upload User Account;
- RDB Server Analysis User Account;

- RDB Server Administrator User Account;
- RDB Process and Architecture Overview (including descriptions of: Step 1: Download and Setup of OCTAVE Automated Tool; Step 2: OCTAVE Automated Tool Execution; Step 3: Transfer Automated Tool Data to RDB Server; Step 4: Transfer Staging Area Data to Risk Database; and Step 5: User Reports Extracted From The Risk Database);
- RDB Server Administrator Quality Assurance Responsibilities;
- Job Description for the RDB Server Manager; and
- Appendices on: Sample Job Description for the RDB Database Manager and SQL Commands For Creating the RDB and RDB Holding Databases.

The manual summarizes the operational and maintenance activities to be performed by the Risk Database (RDB) Server's administrator in order to understand the interconnections of different elements of the RDB application and the RDB Server and to perform the administrative tasks necessary to support them.

2.3.2.10 Transfer RDB to RIMR

Methods/Discussion: The first activity of the RDB transfer to RIMR was to purchase a new computer that would serve as TATRC's RDB server. The Team configured the server with all appropriate system and application software, and tested it, as part of the "Test, Demonstrate, and Enhance the Risk Database" activity described above. When the RDB Server was stable, they performed its security hardening, using the benchmarks published by the Center for Internet Security (CIS). The Team demonstrated the RDB Server to TATRC representatives in a DHIAP Team meeting in early May 2003. TATRC suggested several small enhancements at the meeting, and the DHIAP Team implemented the appropriate changes to the server.

Result: The DHIAP Team implemented the DHIAP RDB Server at TATRC in mid-July 2003.

2.3.2.11 New Task Defined for the Phase III No-cost Extension

Methods/Discussion: For the no-cost extension timeframe, ATI proposed (and TATRC agreed to) augmenting the scheduled RDB tasks in Phase III with a new task to "Support Beta Test of RDB." The task was designed to provide assistance and advice to RDB users—both field users transferring data to the RDB, and central (e.g., TATRC) users who would report and analyze the data. The Team would collect the users' comments and suggestions about RDB functionality, determine changes that should or must be made to the software, and work with appropriate users as necessitated by the changes.

Result: Since no MISRTs had uploaded OAT data to the RDB as of the end of Phase III technical work in August 2003, it was not possible to perform the RDB Beta testing in DHIAP. Responsibility for this activity was transferred in August 2003 to the related ATI-led contract, "OCTAVE Training and Support (OTAS)."[2]

2.4 OCTAVE Comparative Analysis

The OCTAVE comparison task consisted of two major subtasks, *Conduct Comparative Analyses* and *Develop OCTAVE Tailoring Recommendations.* In conducting the Comparative Analyses, the DHIAP Team examined elements of certain external policy and regulatory requirements that have significant impact on MTFs to identify areas where OCTAVE risk assessment activities or results have some relationship to these requirements; the Team then used the findings to recommend ways that MTFs' OCTAVE efforts could help in satisfying certain requirements of the external regulations and ways that the process or results of meeting external requirements could be utilized in completing a site OCTAVE. To develop OCTAVE Tailoring Recommendations, the Team gathered data during Phase III execution (e.g., when training MTF MISRTs, supporting MISRT execution of site OCTAVEs, preparing the comparative analysis reports, etc.) and used the information to develop recommendations for tailoring the OCTAVE Method and/or DoD OCTAVE Training to make them more pertinent to meeting DoD objectives.

2.4.1 Conduct Comparative Analyses

The comparative analysis task was conceived to determine whether a site's execution of the OCTAVE Method, an excellent tool for threat, asset, and vulnerability identification, security policy development, and risk mitigation planning, might also aid in complying with certain other regulations and requirements applicable to the defense healthcare community. The DHIAP leaders believed OCTAVE would help with satisfying some other requirements, but no research on the subject had been performed prior to inception of Phase III. The MTF-applicable requirements and best practice standards selected for the OCTAVE comparison effort are listed below, along with a brief statement of why each requirement applies to MHS/MTFs and a reference to the authoritative source(s) of each requirement:

- DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DIT], [DTS]

  The Defense Information Systems Agency (DISA) has mandated that all DoD organizations use DITSCAP to certify and accredit security of the information technology they utilize (i.e., their networks, systems, and applications) and ensure their use of the technology complies with applicable policies, directives, and laws.[6]

- Security Best Practices as reflected in the NIST Risk Management Guide for Information Technology Systems/NIST SP 800-30 [NST][1]

  MHS and DoD are subject to the Federal Information Security Management Act of 2002,[7] which requires that federal agencies provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. NIST SP 800-30 is one element of the guidance provided by NIST to help agencies meet these requirements.

[6] DoD Instruction 5200.40, December 30, 1997 [DIT], created the DoD IT Security Certification and Accreditation Process (DITSCAP) to be the standard process DoD-wide for security certification and accreditation (C&A) of unclassified and classified information technology to implement the following regulations: DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988; Public Law 100-235, "Computer Security Act of 1987," January 8, 1988; Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996; Director of Central Intelligence 1/16, "Security Policy on Intelligence—Information in Automated Systems and Networks," March 14, 1988; and DoD Directive 5220.22 (references (b) through (f)).

[7] *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the *Homeland Security Act of 2002.*

- Security Standards [SEC] and Privacy Standards [PVC] of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [HPA]

  MTFs and some other MHS organizations are subject to HIPAA requirements. This comparison examines OCTAVE relevance to two components of HIPAA:

  - The HIPAA Security Standards, which provide very specific requirements for protecting the confidentiality, integrity, and availability of PHI[8] that is in electronic form,[9] and
  - The HIPAA Privacy Standards, which mandate that health care organizations provide "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information;"[10] the Privacy Standards require protection of PHI in *all* of its uses and forms—written, electronic, and verbal—throughout a covered entity.[11]

- Accreditation Standards of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) [JCS]

  JCAHO provides "health care accreditation and related services that support performance improvement in health care organizations."[12] MTFs participate in the JCAHO accreditation process to obtain certification of their performance in continuously improving the safety and quality of care provided to patients.

For some of these subjects, the OCTAVE Comparison research could not have been performed as effectively at an earlier time. It was during the Phase III period of performance that a number of the external requirements listed above were finalized—the NIST SP 800-30 in January 2002, HIPAA Privacy Standards "Final Rule" in August 2002, HIPAA Security Standards in February 2003, and JCAHO's "substantially revised accreditation standards"[13] in June 2003.

2.4.1.1 Gather Documentation

Methods/Discussion: The DHIAP Team began gathering source documentation for the DITSCAP, NIST Risk Management, HIPAA, and JCAHO comparison efforts early in Phase III. (See the preceding topic list and the individual report summaries below for additional information on resources that were used.) Where the initial research indicated that the authoritative source to be used in a comparison effort would be changed or updated later in the Phase III timeframe, the DHIAP leaders attempted to schedule the report's research efforts to follow the release of that policy. As a result, the Leaders chose to execute the DITSCAP

[8] PHI (protected health information) is defined by HIPAA as, "individually identifiable health information that is transmitted or maintained using electronic media or any other form or medium." (See "Protected health information," in [SEC] 45 CFR § 160.103, p. 8374, or [PVC] 45 CFR § 164.501, p. 82805.)

[9] Health Insurance Reform: Security Standards; Final Rule (2003) [SEC].

[10] Standards for Privacy of Individually Identifiable Health Information (2000), 45 CFR § 164.530(c)(1) [PVC].

[11] Covered Entity is defined by HIPAA as a health plan, health care clearinghouse, or health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. Note that the following military components are included in HIPAA's "health plan" category: the health care program for active military personnel under title 10 of the United States Code; the veterans health care program under 38 U.S.C. chapter 17; and the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)). (See "Covered entity" and "Health plan" in [PVC] 45 CFR § 160.103, p.82799.)

[12] [JCA].

[13] [JCB].

comparison first, because its requirements were stable and had been in place for several years. The NIST comparison was conducted next, followed by HIPAA Security/Privacy, and then, near the conclusion of Phase III work, the JCAHO comparison.

Result: Research for the comparison reports used the latest versions of the documentation when looking at these requirements that are critical and highly visible in healthcare settings. For DITSCAP, the Team took advantage of Team members' recent experience in conducting DITSCAP Certification and Accreditation reviews. For HIPAA, the Team initially used the proposed rules, but they were able to finalize reporting and recommendations using the final-form regulations. For JCAHO, the Team was able to perform familiarization research using existing standards but format the report to map to the emerging, greatly reorganized 2004 version of the standards. While the reports were prepared by ATI Team members, each one includes the perspectives and expertise of the SEI and TATRC members of the DHIAP Team—in particular using TATRC for input on requirements of the military and SEI for input on criteria and functionality of the OCTAVE Method.

2.4.1.2 Conduct DITSCAP Review

Methods/Discussion: The initial DHIAP Team review of DITSCAP and OCTAVE documentation made a general assessment of their core characteristics, identifying a number of ways that OCTAVE and DITSCAP either overlap or complement each other. To report on this information, the Team had to determine a workable approach for looking at the different dimensions of these methodologies and for organizing the extensive information gathered during the research. Some of the areas of overlap and complement that were identified are listed below.

- Both processes are complex, execute a large number of tasks and subtasks, and require involvement of a number of site staff. DITSCAP requires use of outside experts (e.g., the Certifying Authority), while OCTAVE recommends using outside staff to supplement skills not available from internal staff. Where the two methodologies utilize some of the same site staff, they use them in very different roles and for different purposes.
- OCTAVE and DITSCAP processes use some similar methods and have some goals in common. However, OCTAVE emphasizes how people throughout an organization use and protect its information (while it also conducting a focused investigation of technology-based risks), and DITSCAP emphasizes the technical protection of an organization's information (while also reviewing user-related policy and procedures associated with the system).
- The scope of an OCTAVE is one or more site-selected critical assets (i.e., type(s) of information), including all aspects of the asset's physical and electronic use. The scope of a DITSCAP is one or more computer systems that fall within an "accreditation boundary" established by agreement between the site's designated authority and the external certifier.
- Outputs of OCTAVE are *plans* for improving the site's policy, procedure, and practices related to protecting information assets; the output of DITSCAP is *improved security* for the computer system and a System Security Authorization Agreement that both documents the required level of security and certifies that the required security is in place.
- OCTAVE's documentation of an information asset and its security-related characteristics would be useful to execution of a future OCTAVE that focuses on the same or similar assets. (When using the documentation in the future, the OCTAVE team would have to update it to reflect changes that have occurred in the operational and technical

environments.) DITSCAP's SSAA output should always be current because it is updated both as changes occur and by the next DITSCAP (conducted every three years or when significant change has occurred in the environment).

Since the OCTAVE and DITSCAP processes differ and overlap in so many ways, and since MTFs are required to execute both of them, the Team determined that another research consideration would be to identify how the materials generated by a DITSCAP might be used in an upcoming OCTAVE and, conversely, how the materials generated by an OCTAVE might be useful to an upcoming DITSCAP. The Team ultimately decided to organize the analysis into three areas of investigation: the *process* followed in conducting DITSCAP vs. OCTAVE; the *outputs* produced by the DITSCAP and OCTAVE assessments; and the methods' *guidance* for conducting assessment activities.

In early 2002, the DHIAP Team developed the report's conclusions and considered various ways to organize the extensive research data. The Team compiled an initial draft report that contained a detailed comparison of the methodologies, reviewed it with TATRC, and incorporated the resulting suggestions into the document. Next, the Team used results of the detailed comparison to perform a higher-level assessment of how each method addresses various elements of an organization's operational environment and differences in the meaning and use of their outputs. The Team developed documentation and graphics highlighting OCTAVE's organization-wide emphasis and impact, discussed the initial conclusions of this level of research with TATRC representatives in May 2002, and adjusted some conclusions based on TATRC feedback. At that time, TATRC provided the Team with a copy of "Tailoring OCTAVE to MHS Type Accreditations" for use in report-related research; the document described the approach that the TRICARE Management Activity was using to integrate OCTAVE and DITSCAP activities and apply them to a new system under development.

The Team enhanced and adapted the initial draft DITSCAP-OCTAVE Comparative Analysis report, producing separate volumes that targeted two separate audiences, as follows:

- *Volume 1 – OCTAVE-DITSCAP Comparative Analysis* [ODI] focused on the interests of leaders responsible for deciding when and how to conduct both OCTAVE and DITSCAP at their sites. The volume included an executive summary, graphics to introduce central concepts of the analysis and illustrate key findings.
- *Volume 2 – Support for Site Implementers of DITSCAP and OCTAVE* [ODS] provided detailed instruction, addressing the needs of staff members charged with conducting either DITSCAP or OCTAVE. The volume describes in some detail how a site that is about to execute either DITSCAP or OCTAVE might utilize specific guidance, results, and/or participants from previous execution of the other method.

Report drafts were provided to SEI and TATRC for review and updated to include their applicable recommendations.

Result: The DHIAP research concluded that:

> "The OCTAVE and DITSCAP methodologies are supportive of each other, and a site realizes significant benefit from successful completion of both investigative processes.
>
> - "DITSCAP is a technical certification & accreditation assessment applied to all of a site's systems/networks. In completing its DITSCAP responsibilities, a site ensures that every component of its systems and network infrastructure is secured to the level of risk defined as acceptable in the site's SSAA. The DITSCAP approach utilizes external, independent

reviewers to conduct the investigation in order to ensure objectivity; site staff are used to a limited degree. It performs an extensive technical review of every system that is defined to be within its scope. Documentation of the investigation's goals, interim and final observations, and results are recorded in the DoD-wide standard-format SSAA.

- "OCTAVE is an operational/technical risk assessment applied to assets determined by the site to be most critical to its operation. In completing its OCTAVE, the site ensures that risks to its critical assets are identified and appropriately managed. OCTAVE uses site staff who are extremely knowledgeable of site operations as its leaders in order to ensure that all aspects of asset-related operational activity are considered in the evaluation; outside staff may be used to supplement skills not available in-house. Its vulnerability analyses are conducted for significant components involved in processing critical asset information, each one representing a population of similar components. The investigation's findings about each asset are documented in a standard format, and the organization-level and asset-specific corrective actions that result from the assessment are also published as standard-format documents.
- "By certifying and accrediting the site's systems and networks, DITSCAP provides the means for a site to meet DISA requirements to ensure that technical security is adequate. By examining how the organization manages its critical assets both operationally and technically, OCTAVE ensures that these assets (and others that also benefit from OCTAVE-identified improvement needs) are safely used and technically protected. It will also aid the site in meeting HIPAA requirements for assessing the risks associated with administrative, technical, and physical safeguards for protecting PHI.
- "If sites take advantage of opportunities to share certain elements of each process' execution guidance, previous participants, and/or results, they will realize efficiencies in execution of each process. When a site coordinates its independent execution of OCTAVE's extensive, operationally-oriented investigation and DITSCAP's in-depth technical investigation, the two efforts will produce results that enable a site to significantly strengthen its security posture and ability to safeguard mission-critical information."[14]

The DHIAP Team published "Volume 1–OCTAVE-DITSCAP Comparative Analysis" [ODI] in December 2002; "Volume 2–Support for Site Implementers of DITSCAP and OCTAVE" [ODS] was published in January 2003.

2.4.1.3 Conduct Best Practice Review

Methods/Discussion: The Phase III Technical Development Plan [TD3] originally called for performing this comparison against RFC-2196, "The Site Security Handbook" (a guide to developing computer security policies and procedures for sites that have systems on the Internet).[15] The DHIAP Team began this effort early in 2002 by conducting a high-level review of RFC 2196-requirements. Then, while drafting documentation on how OCTAVE satisfies best industry practices in regard to site information security practices, the Team determined that a comparison of this type would be more useful to the DoD, MHS, and the MTFs if performed using the NIST Risk Management Guide for Information Technology Systems (NIST SP 800-30). The Team Leaders recommended this substitution to TATRC, and TATRC approved the change during the first year of Phase III.

[14] [ODI], pp. ix-x.

[15] The Site Security Handbook is available from http://www.faqs.org/rfcs/rfc2196.html.

The DHIAP Team performed the research using NIST SP 800-30, developed a report draft, and conducted internal reviews of the report content and conclusions. The final draft was provided to TATRC for review.

Result: The DHIAP research concluded that:

> "...OCTAVE is fundamentally equivalent to best practices for an information security risk assessment as described by NIST SP 800-30, and OCTAVE Method Implementation Guidance provides an excellent tool to take the high-level recommendations and guidance found in NIST SP 800-30 to practices. OCTAVE's primary focus on risk assessment activities associated with risk management is an advantage if an organization needs detailed "how-to" instructions on performing and getting high value from an organizationally-led risk assessment. In explaining risk assessment roles and responsibilities, OCTAVE does not limit itself to a particular audience or technical skill set. Personnel inexperienced in assessing risk to information assets within their specific organizations are able to use guidance as explained in the OCTAVE Method Implementation Guides as a means to conduct an information security risk assessment in accordance with industry best practices.
>
> "Though OCTAVE can be tailored to fit the exact outline of NIST SP 800-30, the process of risk assessment is already very similar. The three major differentiators are the asset selection process, inclusion of likelihood in risk determination, and quantitative risk assessment guidance. OCTAVE concentrates primarily on critical assets as a means to direct managerial focus on those information assets that are most critical to the site's mission, as opposed to assessing risk on all information assets regardless of their criticality to the organization. OCTAVE does not include a means of factoring risk based on the likelihood that a particular technical vulnerability may be exploited. Since such probabilistic means of determining risk are inherent to a quantitative risk assessment, OCTAVE does not provide guidance for conducting quantitative information security risk assessments. However, OCTAVE does provide the flexibility to tailor the OCTAVE methodology in consideration of the incorporation of all three differentiators.
>
> "The bottom line from the comparison of OCTAVE to NIST SP 800-30 is that following the OCTAVE guidance will meet the spirit and intent of the NIST guidance for conducting the risk assessment as part of a total risk management program described in NIST SP 800-30."[16]

The DHIAP Team published the "OCTAVE-Best Practices Comparative Analysis (NIST SP 800-30)" [ONS] in June 2003.

2.4.1.4 Conduct HIPAA Review

Methods/Discussion: The DHIAP Team performed some of the research for the HIPAA-OCTAVE Comparative Analysis during 2002 using the proposed HIPAA Security Standards. That work focused on drafting a matrix that matched elements of the proposed Security standards with "best practices" for information security policy and procedure as defined in the *OCTAVE Catalog of Practices* [OCP].[17] When the final Security Standards were published in February 2003, the Team revised the OCTAVE-HIPAA matrix to be appropriate to the Security Standards' final content and sequence. At that time, they were also able to enhance the matrix with additional elements of OCTAVE support for the Standards.

[16] [ONS], p. 19.

[17] The same Catalog of Practice information is available in [OM1] and [OM2], "Volume 15: Appendix A—OCTAVE Catalog of Practices," pp. A-4 – A-23.

Next, the DHIAP Team extended the research to examining OCTAVE support for various PHI protection requirements defined in the final HIPAA Privacy Standards and developing recommendations for how a site might tailor its OCTAVE to address some of these HIPAA requirements. The Team developed a report draft, conducted internal reviews of the report content and conclusions, and provided the draft to TATRC and SEI for review. Both groups provided valuable insight, and TATRC provided with their input the results of some related research they had performed in early 2003 using the proposed version of the Security Standards. The authors incorporated the reviewers' input into the report.

Result: The DHIAP research concluded that:

> "When used to analyze the critical assets that represent a site's manual and electronic repositories of protected health information, the OCTAVE approach to risk assessment is well suited for determining a site's level of compliance with the HIPAA Security Standards and for developing the plans and actions that will greatly improve compliance. When OCTAVE's knowledge elicitation activities gather information on how the site's operational processes manage PHI in verbal and written forms, the OCTAVE will also address a number of PHI protection requirements of the HIPAA Privacy Standards.
>
> "...[The] information protection guidelines provided in the *OCTAVE Catalog of Practices* correspond closely to requirements of the HIPAA Security Standards. The *Catalog's* applicability to the Security Standards can be increased relatively easily by making certain HIPAA-related updates to the *Catalog* (and its related surveys/worksheets), and then using the OCTAVE Methodology to assess and improve the organization's actual compliance with these standards.
>
> ***"Method for Assessing and Improving PHI Protection Throughout the Organization***
>
> "OCTAVE is designed to focus on site-selected "critical" information assets, meaning that a site in need of addressing HIPAA compliance issues can readily address PHI in any of its forms and wherever it is used by the organization. Since the scope of an OCTAVE risk assessment includes both the site's operational environment and its technical infrastructure, the assessment of operational use of PHI is directly complemented by assessment of the technologies and technical practices that support use of PHI. Thus, a site that focuses its OCTAVE risk assessment on its PHI-related critical information assets will evaluate all types of PHI processing, from verbal to written and electronic, in a single risk assessment effort.
>
> "Execution of the OCTAVE approach to risk assessment and implementation of the resulting recommendations (i.e., the Organization Protection Strategy, Risk Mitigation Plans, and Action Items) will permit a site to satisfy a significant number of the HIPAA Security Standards and the PHI protection requirements of the Privacy Standards as well. With some local adaptation to incorporate additional HIPAA requirements in the *Catalog of Practices*, OCTAVE will provide a well-documented methodology for meeting an even greater portion of the Security and Privacy Standards requirements.
>
> ***"Potential for Including Additional HIPAA Privacy Requirements in OCTAVE Scope***
>
> "In its published form, the *OCTAVE Catalog of Practices* aligns well with HIPAA Security Standards. By following OCTAVE's guidance about enhancing the *Catalog* to reflect applicable laws, regulations, and local policy and procedures, a site could add coverage of such Privacy Standards elements as the Notice of Privacy Practices, Authorizations, practices related to Uses and Disclosures, and so on.
>
> "When used "as is," execution of OCTAVE to assess PHI use throughout the organization would identify where and how PHI is used in all of its forms, and would also clarify how the PHI is

> currently protected from exposure. This information establishes the basis for the site to define and implement the necessary administrative, technical, and physical safeguards as stipulated in § 164.530(c) of the Privacy Standards. This same information can also be used as the basis for investigating who can access PHI, and then defining the site's "minimum necessary" policy and ensuring that its implementation conforms with requirements of § 164.502(b) of the Privacy Standards. Finally, for the operational and technical areas investigated using OCTAVE, the post-OCTAVE activities to enhance the site's policies and procedures to reflect improved operational and technical practices will help toward satisfying the Policies and Procedures requirements found in § 164.530(i)(1) of the Privacy Standards.
>
> ***"Summary***
>
> "The robustness of the *OCTAVE Catalog of Practices*, the extensive guidance provided in the *OCTAVE Method Implementation Guide*, and the scalability/adaptability of the OCTAVE process make OCTAVE well suited to assist a site in assessing its existing level of compliance with HIPAA Security Standards and in developing plans to improve the level of compliance. In addition, OCTAVE's emphasis on evaluating and improving operational areas' use and protection of critical assets is well suited to assist a site in meeting the Privacy Standards requirements to provide the necessary administrative, technical, and physical safeguards for PHI in all of its forms—verbal, written, *and* electronic."[18]

The DHIAP Team published "Analysis of OCTAVE Support for HIPAA Security/Privacy Standards" [OHP] in June 2003.

2.4.1.5 Conduct JCAHO Review

Methods/Discussion: In mid-2003, the DHIAP Team began a review of JCAHO accreditation standards to prepare for developing the OCTAVE-JCAHO Standards comparative analysis. Initial activities included reviewing extensive notes provided by TATRC on OCTAVE's applicability to recent JCAHO standards for hospitals, and also meeting with the JCAHO POC at Naval Hospital Charleston (NHC) to gain first-hand knowledge of MTF activities to comply with JCAHO requirements. The NHC POC had firsthand knowledge of the significantly revised standards that JCAHO would soon publish.

On 16 June 2003, JCAHO published on its website copies of the accreditation standards that will be in effect on 1 January 2004. While the overall goals of the accreditation standards remained the same (i.e., to ensure the quality and safety of patient care), the standards were significantly revised and reformatted to consolidate the requirements, eliminate redundancies, reduce paperwork requirements, and ensure their focus on quality and safety. The DHIAP Team used these 2004 standards (the "Hospitals" version) as the basis of the remaining research.

The DHIAP Team performed the research at two levels, first examining OCTAVE support for specific JCAHO accreditation standards and then assessing areas where the processes conducted for OCTAVE risk assessments and JCAHO accreditation might be similar and/or might support each other's requirements. The Team developed a report draft, conducted internal reviews of the report content and conclusions, and provided the draft to TATRC in late July 2003.

Result: The DHIAP research concluded that:

> "...OCTAVE is well suited to provide evidence of compliance with a number of JCAHO Standards, in particular with the standards related to performing the information management

[18] [OHP], pp. 17-18.

> function, performing performance improvement investigations, and using multi-disciplinary groups to analyze and improve performance of care delivery processes. In addition, using the OCTAVE risk assessment methodology, with its best practice standards adapted to be appropriate for the subject of study, is an excellent way to investigate an organization's performance in many other areas of JCAHO concentration."[19]
>
> "Similarities in the JCAHO and OCTAVE approaches to conducting assessments are one way that use of OCTAVE exemplifies compliance with JCAHO principles and even provides evidence of compliance with a number of Elements of Performance of the JCAHO Standards. Both the JCAHO and OCTAVE evaluations are conducted as self-assessments. In both cases, the assessment is conducted by a multi-disciplinary team who have knowledge of diverse areas of the facility and the processes that tie those areas together—for JCAHO's purposes, the sequences of activities associated with care delivery, and for OCTAVE's purposes, the personal interactions, paper trails, and electronic pathways associated with a critical information asset. Both methods focus their assessment efforts on priority areas—when broken down into its elements, the JCAHO priority of "safety and quality of patient care" is not actually so different from the OCTAVE priority of "information assets critical to business continuity." JCAHO assessments use the JCAHO Standards and their Elements of Performance as statements of "best practice" for each function and activity; similarly, OCTAVE uses its *Catalog of Practices* as the benchmark for strategic practices (i.e., policy) and operational practices (i.e., procedure) that should be in place in order to provide appropriate protection to the confidentiality, availability, and security of critical information assets in their paper, verbal, and electronic forms. Finally, both types of assessment require that the organization constantly monitor itself for changes, re-assess itself as needed to preserve compliance with best practices, and continuously improve its methods based on findings of those ongoing assessments.
>
> "In the case of JCAHO, the reward for compliance is accreditation of the healthcare organization; for OCTAVE, the reward is continuing assurance of the confidentiality, availability, and security of critical information assets. Due in large part to the OCTAVE Methodology's approach, recommended staffing, and specific resources such as the *Catalog of Practices*, a healthcare facility is well served in its efforts to achieve JCAHO compliance when it uses OCTAVE as its methodology for conducting risk assessments."[20]

The DHIAP Team published "Analysis of OCTAVE Support for JCAHO Standards" [OJC] in July 2003.

2.4.2 Develop Recommendations for Tailoring the OCTAVE Method

Methods/Discussion: Throughout execution of Phase III activities, the DHIAP Team maintained notes on ways that the OCTAVE Method might be adapted to more closely fit MHS- and DoD-specific requirements. Very important sources of information were the Team's experience with MISRTs and sites' execution of OCTAVE, gained during the ongoing tasks of conducting MHS' OCTAVE training and providing support to site MISRTs as they conducted their sites' OCTAVE risk assessments. Another important source was the research and findings associated with the comparative analysis reports that identified OCTAVE's potential to complement an MTF's DITSCAP, HIPAA, JCAHO, and information security best practices requirements.

[19] [OJC], pp. v-vi.

[20] [OJC], pp. 13.

Results: The DHIAP Team prepared a list of recommendations for tailoring the OCTAVE Method to be more directly applicable to MTF and MHS needs, and provided the report to TATRC in August 2003.

2.5 Biometric Authentication Prototype

In an effort extending from the DHIAP Phase II Business Case Analysis (BCA) research and report, "Effective Authentication in a Medical Environment" [EAU], the DHIAP Team developed and demonstrated a prototype system to study the effects of utilizing biometric technologies for user authentication in an operational MTF environment. The task examined the following hypotheses:

H_{01}: When comparing conventional logon/password to a single type of biometric authentication method in a single context, users never prefer biometrics.

H_{02}: When comparing conventional logon/password to all types of biometric authentication methods in varying contexts, users never prefer biometrics.

The demonstration was designed to determine whether users in operational medical environments will support using a biometric authentication technique (e.g., finger scan, voice recognition, facial recognition, or iris scan) in lieu of the commonly-used password, and also whether characteristics of the operational medical environment (e.g., sound level, use of gloves or facemasks, etc.) influences a user's preference for one type biometric authentication mode over another.

2.5.1 Select Parameters to Evaluate

Methods/Discussion: In October 2001, the DHIAP Team conducted a series of meetings by telephone and in person to identify parameters against which the methods of authentication would be evaluated. They articulated parameters of the operational environments that were to be studied, considered them for inclusion in the evaluation, and then identified the type of evaluation criteria that they would apply. In November 2001, the Team made final updates to the materials, discussed the evaluation parameters and criteria in a meeting with TATRC, and obtained TATRC approval to proceed.

Result: The parameters and evaluation criteria that were selected for evaluation of biometric authentication devices are listed in Table 7. Supporting commentary in the table indicates why the parameter and criteria are relevant to the study.

Table 7 - Biometric Device Evaluation Parameters and Criteria

PARAMETER	EVALUATION CRITERIA	COMMENT
Enrollment	• Success Rate • Time Required • Time Until Re-enrollment	All biometrics require a user to enroll, and since a template ages with time, periodic re-enrollment is necessary.
Authentication	• Accuracy in terms of: ▪ Success/Failure ▪ False Accept Rate ▪ False Reject Rate • Time to Authenticate	Success/Failure and Time to Authenticate can be used to compare biometric methods to password authentication. FAR and FRR can be used to compare biometric methods.
User Acceptance	• Intrusiveness • Ease of Enrollment • Ease of Authentication	Which method of authentication does the user prefer?
Technical Requirements and Maintenance	• Support (Manpower, Cost) • System Requirements • Training • Scalability	Which method of authentication is easiest to support?
Cost	• Cost to Purchase • Cost to Maintain • Recurring Costs	Which is the most cost effective method?
Security	• Assess security primarily in terms of authentication accuracy; however, include other parameters if appropriate.	

2.5.2 Select Biometric Products for Evaluation

Methods/Discussion: The DHIAP Team used a methodology for selecting biometric products for the evaluation that was similar to the approach they followed in DHIAP Phase II to select subjects for its BCAs. This method, based on the Army's Decision Matrix, used weighted criteria, scored each device using the weighted criteria, and used the highest score to determine the "winner."[21] After determining the types of technologies and products available in the marketplace and including in their consideration the products approved and/or recommended by the DoD Biometrics Management Office (BMO), the DHIAP Team identified four biometric products that were representative of currently available technologies.

The DHIAP Team interviewed a number of vendors of biometric devices, including Iridian (provider of iris recognition) and Ultrascan (provider of ultrasonic fingerprints). In addition, they interviewed prospective third party biometric integration vendors, including BioconX, BioNetrix, Keyware, SAFLINK, Vanteon, and Biometrics Solutions Group. Based on these organizations' responses to a questionnaire and results of a follow-on interview pertaining to their ability to assist in the task, the Team selected BioNetrix. Team members conducted a series of conference calls with BioNetrix in December 2001 and January2002 to discuss the DHIAP Biometric Prototype project's requirements in detail.

In a Team meeting in March 2002 attended by TATRC and representatives of the probable trial site, Naval Hospital Charleston (NHC), BioNetrix demonstrated how their product could provide

[21] The method is documented in "General Methodology for Business Case Analysis"[BCA].

the product integration functionality that was needed in the DHIAP Biometric Authentication Prototype. The demonstration showed user verification based on finger scan, facial recognition, iris scan, and proximity card, all running simultaneously on a laptop. Because the demonstration and follow-on discussion of requirements and capabilities were very successful, the Team subsequently established formal non-disclosure and software trial agreements with BioNetrix for using their product in the DHIAP Biometric Authentication Prototype.

Result: The DHIAP Team determined that the following types of biometric devices should be included in the scope of the investigation: finger scan, iris recognition, facial recognition, and voice recognition. In addition, they concluded that they would use BioNetrix as the vendor for authentication device integration support.

2.5.3 Develop the Prototype and Data Collection Requirements, Specifications

Methods/Discussion: During a DHIAP Team meeting in January 2002, the Team reviewed and assigned responsibility for developing the requirements specifications, the operational test plan, and the data collection plan. The CIO from NHC attended these meetings, and was most helpful in adding a user perspective to the Team's planning efforts. Table 8 lists the basic assumptions that were determined to be central to the prototype's design.

Table 8 - Basic Design Assumptions of the Biometric Prototype

FACILITY-RELATED ASSUMPTIONS	TECHNICAL ASSUMPTIONS
• The system will be transparent to, and have no effect on, existing MTF networks or systems (e.g., CHCS). • The site's password authentication capabilities will remain available during the demonstration as backup • MTF operational environments selected to participate in the demonstration will include those considered in the Phase II authentication Business Case Analysis (e.g., administrative area, laboratory, nursing station, etc.)	• The prototype system will be capable of authenticating a user in one of four biometric modes (finger, voice, face, iris), as well as password, in a given operational environment. • Authentication to the biometric prototype will not take place until the user has successfully authenticated to the workstation/network, the screensaver (set to a short time) has activated, and the user initiates an attempt to re-authenticate to the screen saver's lockout. • Authentication will be by *verification* (where the user claims an identity and the system verifies it) rather than *identification* (where the system matches the user's biometric input against a database of all users' characteristics to determine identity)

Team members met with TATRC in October-November 2001 to further develop and confirm user requirements for the demonstration effort. Next, they used these requirements, along with knowledge gained from the technology assessments performed in the preceding "Select Biometric Products for Evaluation" task, to develop the functional requirements and technical specifications for integrating the prototype's biometric devices, data collection software, and database repository.

The Team concluded that the sequence of events, or "stages" of the demonstration would be executed as follows:

- **Stage 1** - Equip a PC with *one* biometric mode/device and password for user authentication and, upon activation of the screen saver, re-authentication. Give users a choice of re-authenticating with either the biometric or the password. Execute the data collection effort by rotating through each biometric mode on the PC (each installed for a set time period such as one week) in each of up to four operational environments.

- **Stage 2** - Equip a PC with *up to four* biometric modes and password for user authentication and re-authentication. Direct the user, who had been trained in Stage 1 on each method of authentication, to select the method of authentication he/she prefers to use, thereby providing user acceptance data. Execute the data collection effort by rotating the PC through each of the four operational environments.

The Team also decided that the technical approach for supporting the demonstration would be to implement a screen saver on the Windows NT/2000 workstation and set the screen saver for quick activation so that it would rapidly conclude a user's access. This would make it necessary for a user to re-authenticate using either a biometric device (or, as a backup, a password) in order to re-open the system for active use. (Passwords would remain available as fallback to ensure that a biometric authentication failure did not unduly interfere with operations.)

The Team defined the functional requirements and technical specifications necessary to support interfacing with the NT/2000 screen saver log-on and the means of capturing parametric data. They planned to leverage vendor expertise as much as possible throughout the development process and coordinate with the BMO to ensure the prototype would satisfy applicable DoD standards.

Result: Requirements and specifications developed for the biometric authentication prototype technology were based on an assessment of the user requirements. The resulting *Functional Capabilities* (describing how the system would work and what it should do) developed for the system's two primary components, GUI and the data collection, were the following:

- **GUI Requirements:** Prompt the user through the enrollment process, prompt the user to indicate how he/she would like to authenticate (biometric or password), and provide the system's administrators (the DHIAP Team) with a means to access the collected data.
- **Data Collection Requirements:** Collect data on the evaluation parameters (see Table 7). Data collection activities concealed from user view were to include criteria such as authentication accuracy, time to enroll, time to authenticate, usage rate, etc.; data collection activities that would be obvious to the user were to provide a survey instrument to capture data relating to parameters such as user acceptance.

The resulting *Functional Attributes* to be considered during design and development of the biometric prototype were the following:

- **Availability:** While biometric products might individually cause false rejects of authorized users, the biometric prototype as a whole should not impede authorized users from accessing applications needed to conduct operations in the environment; passwords should be available if the user is unable to authenticate with a biometric method.
- **Efficiency:** The biometric prototype should run in a manner that is transparent to the user in terms of workstation resource (storage, memory, CPU) requirements; minimum workstation configuration requirements should be provided in the site installation plan.
- **Flexibility:** The biometric prototype design should consider the possible future need to integrate other biometric products.
- **Integrity/Security:** The biometric prototype should maintain protection of the data stored/processed on the workstation by not degrading the security features of the

workstation; only administrators should be able to view data collected by the biometric prototype, and that data is to contain no user-specific information.

- **Interoperability:** The biometric prototype should not impede the interoperability of other applications.
- **Reliability:** The biometric prototype should be fully tested before any site installation; while individual biometric products might fail according to their own reliability capabilities, the biometric prototype as a whole should not fail to the extent that a workstation reboot could not correct the problem.
- **Robustness:** If the individual biometric method of authentication were to fail to authenticate an authorized user, password authentication (and conceivably other biometric modes) should be available.
- **Usability:** Some degree of user learning and user enrollment would be a requirement for use of each biometric method; however, user acceptance should be a key parameter in comparing methods of authentication.

The resulting *Technical Requirements* identifying what would be technically necessary to support the functional capabilities included the following:

- **General Technical Requirements:** Use Windows NT/2000 as the prototype's operating system, and integrate biometric modes to the operating system for authentication; implement integration of biometric devices using third-party software.
- **GUI Technical Requirements:** Integrate the GUI to the operating system's screen saver authentication function, and integrate the GUI to biometric modes and/or to the third party software.
- **Data Collection Technical Requirements:** Use Microsoft Access for database functionality unless the data is collected in some other readily available and readable form (such as a data delimited ASCII text file) by the vendor-provided software that comes with the biometrics device(s), and integrate data collection with utilization of the biometric modes of authentication and with password authentication.

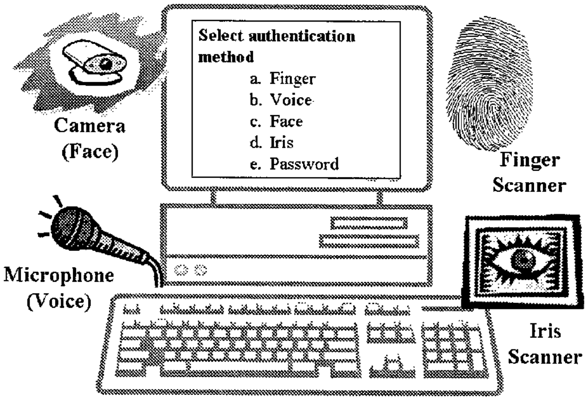


Figure 4 - Biometric Authentication Prototype Workstation

2.5.4 Design and Develop the Prototype

Methods/Discussion: The DHIAP Team designed and developed the Biometric Authentication Prototype and tested the implementation in a laboratory environment. Components of the prototype system (depicted in Figure 4) included a Windows NT/2000 workstation with a variety of biometric devices attached for finger, voice, face, and iris authentication. Software developed to support the prototype demonstration focused on capturing information pertaining to the evaluation parameters (e.g., success/failure of authentication, time required to authenticate, etc.) each time a user made an attempt to log on to the demonstration system. Support for information capture was designed to support the Team's ability to make quantifiable comparisons of the methods.

The design developed for the prototype included the following components:

- GUI design with draft of the screen format to be used;
- Design for the local database (e.g., length of field, alpha vs. numeric input, range of acceptable values, etc.) for collecting data;
- Design for the interfaces external to the software and between/among the vendor's biometric products;
- Draft user documentation; and
- Preliminary test procedures.

Upon completion of the design, the Team conducted a design review with TATRC and made minor updates to the design based on results of the meeting.

Result: Following successful completion of internal testing, the DHIAP developers demonstrated the biometric prototype in August 2002 to NHC senior IT staff and the DHIAP Team. The demonstration used a prototype version that included server with control and database software and client machines with all four biometric devices fully operational.

2.5.5 Collect Data in Laboratory Setting

Methods/Discussion: After testing the system to ensure it met all technical requirements, the DHIAP Team began testing its operation in a simulated MTF operational environment in the ATI DHIAP laboratory. Using drafts of instructions developed for MTF staff to use during the demonstration, the DHIAP Team enrolled a number of ATI employees on all four of the prototype's biometric devices. ATI enrollees simulated what was expected to occur during the demonstration at NHC by regularly signing on to the workstation, allowing the workstation to time out/display the screen saver, and attempting to re-authenticate using the various biometric technologies.

Result: The data collection testing effort met its primary goal of establishing a baseline of data using a controlled operational environment with cooperative users. It also provided an opportunity for the DHIAP Team to refine and rehearse procedures for user enrollment and verification prior to beginning work with the trial site, making minor enhancements to software and documentation as necessary. The Team succeeded in testing against equipment configurations that might be found at the trial site, and they were able to develop installation procedures/guidelines and enhance details of the site installation and data collection plan. The Team's successful demonstration of these internal tests to NHC senior IT staff led to confirmation that NHC would begin executing the biometric prototype trials immediately.

2.5.6 Recruit a Site

Methods/Discussion: The goal of the trial site recruitment effort was to be able to assess the effects of an operational medical environment on use of the biometrics technology. (For example, the BCA findings noted that voice recognition is a poor choice in an outpatient clinic because of the background noise; while this seemed to make sense and undoubtedly applies to many voice recognition products, the DHIAP Team believed should be tested and validated with hard data. Similarly, the vendor of iris recognition technology claimed to be capable of capturing good data even when a person wears glasses—but could that success be ensured for wearers of protective goggles and/or surgical loupes?) The DHIAP Team's backup plan, to be executed if it were not possible to enroll a medical site, was to obtain data by simulating various medical operational environments in a laboratory setting.

Early in Phase III, the DHIAP Team contacted representatives of an MTF local to the ATI developer site, the Naval Hospital Charleston (NHC), and asked if they would participate in the biometric demonstration. DHIAP Team members briefed the facility Commander and senior staff (including the Chief Information Officer) in November 2001, and NHC leadership expressed interest in learning more about the effort. In mid-January 2002, the NHC Chief Information Officer (CIO) and a staff member participated in a planning session that included a high level demonstration of the capabilities that the team expected to include in the biometric prototype. During that meeting, the NHC Information Technology (IT) leaders made valuable contributions to the Team's plan for executing the demonstration—suggesting particular areas of the medical facility where unique conditions might demand certain types of biometric devices and prove others to be of little use.

In late August 2002 when the biometric authentication prototype was undergoing final testing in the development laboratory, NHC IT representatives visited with the Team for a demonstration of how medical facility staff would be enrolled in the system and then utilize the system. NHC's positive response to the demonstration enabled the DHIAP Team to confirm dates of installing equipment at NHC and the timeframe of the demonstration. The group also confirmed the plans for rotating the demonstration equipment from its initial installation location (the IT department where NHC IT staff would gain familiarity with the equipment and processing) to the various operational departments that would perform testing. In a meeting held in early September 2002, the DHIAP Team and NHC completed detailed planning for logistics, training, and delivery approach for the NHC implementation of the biometric prototype.

Result: NHC agreed to be the trial site for demonstration of the biometric authentication prototype. Plans were made to install equipment at NHC and execute the demonstration beginning in mid-September 2002.

2.5.7 Install Prototype at the Site

Methods/Discussion: The DHIAP Team developed the Installation and Operation Plan for the prototype trials in cooperation with NHC, and then executed it. Together, they installed the BioNetrix server and a client in the IT area and trained IT staff to use it. During 18-27 September 2002, the NHC IT staff members became familiar with the equipment and gained confidence that the demonstration would be no impact on the facility's network. On 30 September 2002, the DHIAP Team installed one biometric device and password for user authentication on the PCs of four representative users. The implementation offered users the choice of authenticating with either the biometric or the password. The Team trained the NHC users to authenticate themselves using the DHIAP equipment, and arranged to visit NHC regularly to check on equipment operation and move biometric devices from one workstation to the next according to Plan.

Result: Prototype installation was completed according to plan. After testing the biometric prototype in their work area, NHC IT staff approved and assisted in the 30 September 2002 activities to install the prototype on workstations of the users selected to participate in the demonstration.

2.5.8 Collect Data in Operational Environment

Methods/Discussion: Throughout the demonstration's Stage 1, the DHIAP Team worked closely with NHC staff and the integration vendor, BioNetrix, to resolve the issues as they arose. All parties worked cooperatively to identify and implement solutions. At one point in the Stage 1 work, a member of the BioNetrix management team visited NHC with the DHIAP Team to observe the study. As testing progressed, the Team found it necessary to slightly modify the original plan for conducting the study. However, they succeeded in capturing data from each environment and for each device as planned.

Upon completion of the demonstration trials, DHIAP Team retrieved all biometric devices, uninstalled all BioNetrix client and server software, ensured that the client workstations were returned to proper operation, and photographically documented the environments used in the demonstration. Also, in accordance with the Data Collection Plan, the Team surveyed the users to obtain users' impressions and suggestions for the project's final report.

The Team encountered some challenges during the trials. Some of the users were "goats"–a term used in the biometric industry to describe a user who is unable to use a certain type of device (e.g., a user with worn fingerprints). One user was unable to use his PC frequently enough to provide adequate data, so the Team replaced that user with another individual who used the PC more often. Also, as the Team had expected from its DHIAP Phase II work, some user environments were unfavorable for certain biometric authentication methods—for example, lighting conditions severely impacted facial recognition, and background noise affected the usability of voice recognition.

Result: Initial analysis of raw data from the NHC trials indicated that biometrics were not highly effective for user authentication in a medical environment. The voice and face recognition, in particular, performed poorly—both methods being highly influenced by elements such as the environment's noise and lighting. When operational, the iris recognition performed better. Fingerprint scanning seemed to perform the best. Users' feedback concerning the individual modes supported these technical findings, but, surprisingly, most users expressed a positive outlook about biometric authentication eventually replacing passwords.

Due to the less-than-positive results of the NHC trials, the DHIAP Team decided to conduct additional trials at ATI. They hoped to obtain improved results by using an environment that was considered "highly cooperative." Interestingly, the trials in the more controlled ATI environment produced results that corresponded closely to the NHC results.

2.5.9 Compile Data and Report

Methods/Discussion: The DHIAP Team began the data analysis effort by removing "bad" data (e.g., data collected during the Team's internal testing and equipment installation at NHC) from data collected during the actual authentication trials at NHC. The Team then classified and analyzed the data and drafted a report of the study's findings. They provided the draft to the NHC CIO for review and comment and received positive feedback with no changes to the report's content. The Team also used materials associated with the demonstration to construct a presentation on the demonstration and its results.

Result: The Team's report on the demonstration effort, which referenced both the formal trials at NHC and the less formal trials conducted at ATI, concluded the following:

> "While biometric authentication may not yet be mature enough for enterprise-wide deployment "out of the box," this study did find evidence that biometric authentication could one day replace passwords and that certain biometrics are more appropriate than others depending on the user environment. In this study, fingerprint and iris recognition performed far better than voice and face recognition. The results of this study can support the decision-making process for implementation of an effective means of authenticating users of medical information systems. While it is based on analysis of the biometric authentication technologies used at military medical treatment facilities, it is equally applicable to other military and non-military environments."

The DHIAP Team published "Biometric Authentication in a Medical Treatment Facility" [BAM] in June 2003. The analysis and findings documented in the report was also the subject of a presentation made by DHIAP Team members at the 2003 Annual Conference of the American Telemedicine Association in May 2003.

3 Conclusions

DHIAP accomplishments have significantly improved the ability of the Military Health System (MHS) to protect its information resources. The DHIAP Team has developed and proven a methodology for assessing risk to critical information assets, developed a course and materials for training individuals to conduct risk assessments, and developed a train-the-trainer course that will support the military's need to develop new risk assessment trainers and leaders from among their ranks. DHIAP Team members personally trained over 600 representatives of the 170+ military medical facilities worldwide to perform risk assessments, and they have implemented and served as the knowledge resource for a centralized support infrastructure that provides timely guidance and assistance to MTF sites' risk assessment teams. The Team developed an automated tool to support the labor-intensive data capture and reporting activities of a site's risk assessment, and they implemented at TATRC a centralized database facility to aggregate the results of all MTFs' risk assessments and analyze them using a state-of-the-art query and analysis toolset. In related research efforts, the Team investigated and reported on how site execution of the risk assessment methodology could help them comply with certain other mandates, such as DITSCAP, HIPAA regulations, JCAHO accreditation, and meeting "best practice" guidelines for site information security practices. In a DHIAP technology demonstration effort, the Team assessed and reported on the viability of currently available biometric technologies to augment or replace MTFs' existing use of passwords for user authentication.

3.1 Technical Management

The DHIAP leaders worked closely with TATRC throughout Phase III to ensure that plans and schedules for Phase III work efforts kept pace with the changing needs and schedules of DoD and MHS, in particular with regard to MTF compliance with the HIPAA Security Standards. They have also ensured that the interim and final work products delivered by DHIAP meet or exceed the government's high expectations for quality.

3.2 Deploy OCTAVE

Phase III activities to deploy the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method throughout the Military Health System included development and delivery of training, as well as development, support, and use of a web-based application for supporting trained OCTAVE users.

The deployment effort began with making enhancements to the existing approach to conducting OCTAVE training and then conducting that training for the military's Medical Information Security Readiness Teams (MISRTs) at the TRICARE Management Activity HIPAA Summit 2001. The effort continued with improving the training approach based on both the Summit experience and the recent release of Version 2.0 of the OCTAVE Method. Using the result of these activities, the DHIAP Team trained MISRTs from around the world, equipping them to begin meeting requirements of the HIPAA Security Standards by conducting OCTAVE risk assessments at their facilities. The OCTAVE approach of evaluating how critical assets are handled throughout the organization (regardless of whether the assets are being used in electronic or physical/verbal forms) and improving policy and procedure for protecting the assets also served to help MTFs improve their compliance with the Privacy Act of 1974[22] and with HIPAA Privacy Standards requirements for protecting information with appropriate administrative, technical, and physical safeguards.

Another portion of this effort produced the OCTAVE Information Center (OIC), a centralized support capability that allowed the DHIAP Team (and later the military) to provide guidance to MISRTs as they execute site OCTAVEs. The website-based facility lets MISRTs enter questions for the support staff, allows the support staff to collaborate as necessary on a response, and permits the support staff and MISRT member to continue their communication via direct email. It also provides knowledge resources such as FAQs (guidance based on Frequently Asked Questions that users can scan to learn from the issues and experiences of others), a Message Board for discussion of OCTAVE-related ideas and issues, write-ups of Lessons Learned by sites that are working with OCTAVE, and links to other resources that might be of interest to OCTAVE users. A unique capability of the OIC is its use with the OCTAVE Tools. As described below, the OIC is the conduit for MISRTs to download a copy of the PC-based OCTAVE Automated Tool for use during their OCTAVE and to upload site OCTAVE results to the Risk Database for cross-site analysis. The DHIAP Team members supported the OIC throughout Phase III and, through this activity, provided support to MISRTs and gathered ideas for enhancing OCTAVE, its training, and its support mechanisms.

Finally, this effort produced an OCTAVE Train-the-Trainer course. The course was adapted to the military's needs and enhanced with MHS-specific teaching examples, trainer materials, and student materials. The course was turned over to TATRC so that the military's deployment of the OCTAVE Method for conducting risk assessments will continue long after the close of DHIAP Phase III activities.

In DHIAP Phase III, the Team trained over 600 military medical professionals to conduct OCTAVE Method risk assessments. This accomplishment increased the overall level of security awareness among clinicians, patient administrators, and Information Technology staff at every military MTF, and also increased the effectiveness of procedures that all sites follow when dealing with sensitive information. Recognition of the value of a self-directed methodology for conducting risk assessments as represented by OCTAVE has gathered momentum, and OCTAVE is being used within DoD not only as the approved method for conducting risk assessments to support meeting HIPAA requirements, but also as a mechanism for reducing risk when planning complex systems and infrastructures.

3.3 OCTAVE Tools

This technical development effort produced two OCTAVE-related software tools, the OCTAVE Automated Tool (OAT) and the Risk Database (RDB). Each tool is useable and useful on its own. When used together, however, they will greatly enhance benefit that DoD/MHS derives from employing the OCTAVE Method in all medical facilities.

- OAT provides PC-based support for MISRTs' OCTAVE execution at their MTFs. Available to sites via download from the OCTAVE Information Center, the OAT reduces the effort of the OCTAVE "scribe" activities to capture data, ensure it is appropriately recorded for each affected asset and OCTAVE Method circumstance, and produce reports

[22] 5 USC § 552A.

that are prerequisite to executing each new step of the OCTAVE. Through extensive edits and other software capabilities, the OAT also helps to improve the quality of the data that is captured at a site. Because it reduces the considerable burden of manually managing the large volume of information gathered during each execution of an OCTAVE, the OAT is key to ensuring broad acceptance and use of the OCTAVE Method throughout the DoD medical community.

- The RDB is a central repository where OCTAVE information and results from sites throughout DoD/MHS can be assembled and analyzed. Individual MTFs can post their OCTAVE data and results to the RDB through an interface that is part of the OCTAVE Information Center functionality. The interface moves the data through a series of edits that check for completeness, and then posts the data to the RDB. RDB security capabilities control who may access the data and what they can do with it. RDB functionality includes a variety of standard reports and an ad hoc reporting capability that allows authorized RDB users to query and analyze the data in any number of ways. RDB-based analyses of the data accumulated from many MTFs will allow the appropriate DoD higher echelons to gain an understanding of information threats and vulnerabilities across the MHS and protection strategies that have been implemented at the sites to address these vulnerabilities. They will be positioned to monitor security assessment activity across all MTF sites and determine the level of improvement in MHS' security posture over time. In addition, higher echelons will be able to determine how effectively sites are using OCTAVE to identify and address their risks and use this information to improve resources available to the sites and/or enhance and adjust MHS OCTAVE training.

As of the end of Phase III, the OAT production version had been packaged and made available for MTFs to download from the OIC. The RDB had been tested, refined, and implemented at TATRC for gathering MTF data as it is made available. Both OCTAVE Tools have online and print-format documentation appropriate for their use, support by military personnel, and ongoing maintenance. Also, both Tools had undergone a preliminary version of DITSCAP testing to ensure that their documentation and software would be ready to undergo formal certification and accreditation by the military.

3.4 OCTAVE Comparative Analysis

When the DHIAP Team compared OCTAVE with certain other regulatory and professionally mandated requirements that MTFs must deal with, they judged OCTAVE to be both useful for supporting the external requirements and the source of tangible results and documentation that would assist the site with compliance.

- The Team judged OCTAVE to be consistent with and exemplary of information security "best practices" as recommended in NIST SP 800-30, the "NIST Risk Management Guide for Information Technology Systems."

- The Team determined that OCTAVE's baseline for information protection, the "OCTAVE Catalog of Practices," reflected requirements of the HIPAA Security Standards to a significant degree, only falling short in isolated, healthcare-specific requirements such as requirements relating to the HIPAA-mandated Business Associate contracts and a few other requirements (such as ensuring that written policies and procedures are retained for a minimum of six years) that could be readily satisfied by enhancing the Catalog. They also concluded that OCTAVE's emphasis on gathering threats, vulnerabilities, and security concerns from knowledgeable staff throughout the organization could help a site comply with the HIPAA Privacy Standards' health information privacy and "minimum necessary" requirements.

- The Team found that JCAHO's emphasis on using multi-disciplinary teams of site staff to assess and improve a medical facility's procedure and practice is mirrored in OCTAVE's recommendations for composition of the OCTAVE Analysis Team and its approach to information-gathering. Both methods focus the self-assessment on priority areas, compare site practice to a "best practice" standards for the subjects of study, and require continuous self-monitoring and improvement. In addition, they noted that a site's execution of the OCTAVE Method provides evidence of compliance with a number of JCAHO standards and elements of performance.
- The Team found that, while both OCTAVE and DITSCAP are designed to improve a site's overall security posture and increase site information security awareness, the assessments serve distinctly different purposes—DITSCAP ensuring security of technical information systems and their use, and OCTAVE ensuring information protection in the organization's operational processes and use of systems. The Team identified a number of circumstances where sites executing either OCTAVE or DITSCAP could utilize elements of the process, guidance, and/or outputs from the other methodology. They concluded that a site would receive maximum benefit by executing both methodologies.

In this task's development of tailoring recommendations for the DoD-MHS version of the OCTAVE Method, the Team synthesized knowledge gained from conducting MHS' OCTAVE training, providing support to site MISRTs through the OCTAVE Information Center, and identifying OCTAVE's potential to complement an MTF's DITSCAP, HIPAA, JCAHO, and information security best practices requirements. They developed recommendations for adapting the "classic" OCTAVE to be more directly applicable to circumstances of military MTFs.

3.5 Biometric Authentication Prototype

This technical effort constructed a prototype from generally available commercial products and demonstrated the utility and limitations of current and emerging biometric technologies in a medical environment. The DHIAP Team started with constructing and testing a prototype system for user authentication that supported finger scan, iris scan, face scan, and voice recognition. Trials of the prototype in a military medical facility tested the usability of these authentication approaches in the diverse physical environments characteristic of a medical facility—where there is significant noise, where rubber gloves are in use, where hands might be covered with lotion or talc, where goggles and/or masks are used, etc.

Side-by-side testing of the different authentication modes in operational settings captured unbiased, vendor-neutral data in a military medical facility environment. The study found that unique aspects of the user environment made certain biometric authentication approaches more desirable than others, leading to the conclusion that a site's implementation of biometrics must consider the physical site characteristics, and even the user attire, of each environment where they will be installed. Based on the nature and number of difficulties encountered in both installing and using the biometric authentication devices and systems, the Team concluded that the technologies were not yet mature enough for enterprise-wide deployment. They also noted that they found evidence that biometric authentication could one day replace use of passwords.

4 References

[ANN] Andrews, A, et al. (2002, October 14). Defense Healthcare Information Assurance Program (DHIAP) Final Report: Annual Report for Year 1 of DHIAP Phase III. (ATI IPT 02-01. DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute.

[BAM] Pellissier, S., Simon, S., & Stinson, J. (2003, June). Biometric Authentication in a Medical Treatment Facility. (ATI IPT Technical Report 03-3, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[BCA] Pellissier, Stephen V., et al. (2001, May). General Methodology for Business Case Analysis. (ATI IPT Technical Report 01-04, DAMD17-99-C-9001). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[DIT] DoD Instruction 5200.40. (1997, December 30). DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP). Available from: http://www.dtic.mil/whs/directives/corres/html/520040.htm.

[DTS] DoD 8510.1-M, (2000, July 31). DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP) Application Manual. Available from: http://www.dtic.mil/whs/directives/corres/html/85101m.htm.

[EAU] Pellissier, Stephen V., et al. (2001, January). Effective Authentication in a Medical Environment Business Case Analysis. (ATI IPT Technical Report 01-01, DAMD17-99-C-9001). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[FNL] Andrews, Archie, et al. (2001, June; revised 2001, October). Defense Healthcare Information Assurance Program (DHIAP) Final Report: DHIAP Phases I and II. (ATI IPT 01-05, DAMD17-99-C-9001). North Charleston, SC: Advanced Technology Institute.

[HPA] Health Insurance Portability and Accountability Act of 1996. Available from: http://cms.hhs.gov/hipaa/.

[JCA] Who Is The Joint Commission on Accreditation of Healthcare Organizations? Joint Commission on Accreditation of Healthcare Organizations (JCAHO). Retrieved 27 August 2002, from: http://www.jcaho.org/general+public/who+jc/who+is+the+joint+commission.htm.

[NST] Stoneburner, G., Goguen, A., & Feringa, A. (2002, January). Risk Management Guide for Information Technology Systems (NIST SP 800-30). Washington, DC, National Institute of Standards and Technology, Department of Commerce. Available from: http://www.mirrors.wiretapped.net/security/info/reference/nist/special-publications/.

[OCP] Alberts, C. & Dorofee, A. (2001, October). OCTAVE^{SM} Catalog of Practices, Version 2.0 (Technical Report CMU/SEI-2001-TR-020). Software Engineering Institute, Carnegie Mellon University. Available from: http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html.

[ODI] West, S., Crane, L., & Andrews, A. (2002, December). OCTAVE-DITSCAP Comparative Analysis. (ATI IPT Technical Report 02-2, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[ODS] West, S., Crane, L., & Andrews, A. (2003, January). Support for Site Implementers of DITSCAP and OCTAVE. (ATI IPT Technical Report 03-1, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[OHP] Crane, L., West, S. & Andrews, A. (2003, June). Analysis of OCTAVE Support for HIPAA Security/Privacy Standards. (ATI IPT Technical Report 03-2, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[OJC] Crane, L.. (2003, July). Analysis of OCTAVE Support for JCAHO Standards. (ATI IPT Technical Report 03-5, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[OM1] Alberts, C. and Dorofee, A. (2001, January) Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Method Implementation Guide, Version 1.0. Software Engineering Institute, Carnegie Mellon University. Available from: http://www.aticorp.org/info_prot.htm.

[OM2] Alberts, C. & Dorofee, A. (2001, June) Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Method Implementation Guide, Version 2.0. Software Engineering Institute, Carnegie Mellon University.

[ONS] West, S. & Andrews, A. (2003, June). OCTAVE-Best Practices Comparative Analysis (NIST SP 800-30). (ATI IPT Technical Report 03-4, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[PVC] Standards for Privacy of Individually Identifiable Health Information. (2000, December 28). Title 45 Code of Federal Regulations Parts 160 and 164, Federal Register, 65 (250), 82461. Final Rule. (2002. August 14). Federal Register, 67 (157), 53182. Available from: http://www.hhs.gov/ocr/hipaa/finalreg.html.

[RDA] Stinson, J. (2003, July). Risk Database Administrator's Operation and Maintenance Manual. (ATI IPT Technical Report 03-5, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute. Available from: http://www.aticorp.org/info_prot.htm.

[SEC] Health Insurance Reform: Security Standards; Final Rule. (2003, February 20). Title 45 Code of Federal Regulations Parts 160, 162, and 164. Federal Register, 68 (34), 8334. Available from: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf.

[TD3] Andrews, Archie D., et al. (2002, March, initially published 2001 October). DHIAP Phase III Technical Development Plan-Baseline. (ATI IPT, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute.

[TDR] Andrews, Archie D. (2002, December 9). Revised Program Plan—DHIAP III, 9 December 2002. (CNTS-WW1210-31696 2002 December 10, DAMD 17-01-C-0048). North Charleston, SC: Advanced Technology Institute.

THIS PAGE INTENTIONALLY LEFT BLANK

5 Appendices

Appendix 1 – Overview of DHIAP Phases I and II

Appendix 2 – MTF Support Log

Appendix 3 – OCTAVE-Trained Staff Who Have Enrolled for OIC Access

Appendix 4 – DHIAP Phase III Technical Development Plan

Appendix 5 – Revised Program Plan—DHIAP III, 9 December 2002

Appendix 1 – Overview of DHIAP Phases I and II

Note: This material has been adapted from the DHIAP Phase I-II Final Report.[23]

DHIAP Phase I

Technical Assessment Task

The Technical Assessment Task was designed to evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities. Its major activities are depicted in Figure 5. Using a methodology developed and used by the Software Engineering Institute (SEI) called the Information Security Evaluation (ISE), DHIAP Team members experienced in system security and in healthcare operations analyzed the information protection procedures and capabilities of selected military MTFs. Upon completion of each ISE, the Team provided the site with a summary of the security issues and site security exposures that were identified, along with recommendations for improving its information security posture. When both ISEs had been completed, the Team analyzed similarities and differences in findings at the sites and prepared a "composite" report of findings and overall recommendations for improving protection of the military's healthcare information assets.

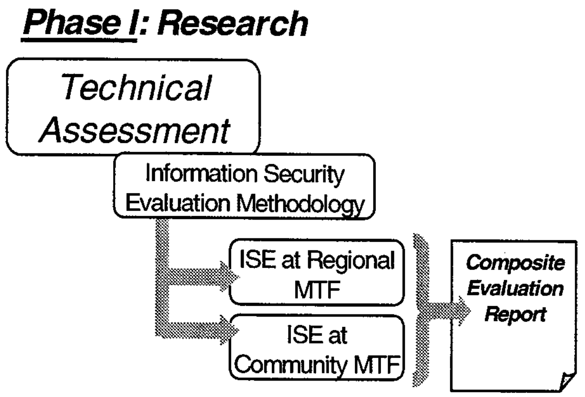


Figure 5 - Overview of Technical Assessment Task

This analysis found that the security of patient information in the military medical system can be compromised and is at risk. Vulnerabilities at the local MTF level are caused, in part, by the centralized selection, administration, and maintenance of mandated health information systems. While concerted effort on implementation of current military regulatory guidance will mitigate some of the identified vulnerabilities, others that are beyond the site's capability and authority to address will require action on the part of higher echelons. Further, the military health system will face additional exposure when assessed against the emerging standards for privacy of individually identifiable health information that will be required under the pending legislation and regulatory guidance of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[24]

While the goal of the Technical Assessment Task was to identify technology solutions for vulnerabilities in the military's ability to protect healthcare information, it became evident to the DHIAP Team that a multi-faceted solution is necessary. Neither technology enhancements nor

[23] [FNL]

[24] *Health Insurance Portability and Accountability Act of 1996.* Public Law 104-191. August 21, 1996. URL: www.aspe.os.dhhs.gov/admnsimp/pl104191.htm.

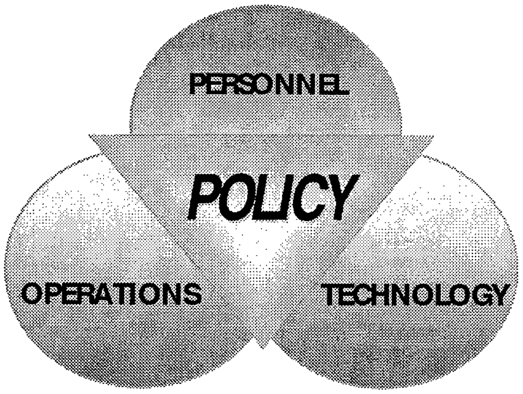
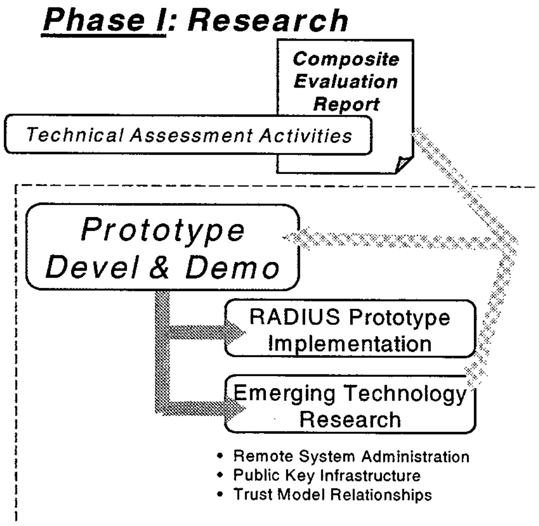


Figure 6 - Key Elements of Information Assurance

carefully planned changes to current policies and procedure can alone solve current problems. Rather, as depicted in Figure 6, the observed state calls for an approach that encompasses policy, operations, personnel, and technology. Emphasis on any single area without regard for the other areas will not produce the desired results. Therefore, any plan to address identified information assurance issues should start with a vision of where information assurance fits into the command's policy and priorities. A comprehensive Information Assurance Policy that addresses information security in relation to operational requirements is needed to direct and guide the military's information protection activity. As policy is promulgated to the diverse organizations involved with military health information from the agencies that select and implement systems to the MTFs that treat patients, it should be used to provide a unifying influence for defining operational, personnel, and technology changes that will ensure protection of military healthcare information.

Prototype Development, Demonstration, and Transition Task

Figure 7 - Overview of Prototype DD&T Tasks



Phase I: Research
Composite Evaluation Report
Technical Assessment Activities
Prototype Devel & Demo
RADIUS Prototype Implementation
Emerging Technology Research
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships

The purpose of the "Prototype" Task was to validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems, and then implement security solutions for evaluation within the military medical community. As depicted in Figure 7, the DHIAP Team used findings of the Technical Assessment Task's ISEs to identify an information technology to be studied in this task and to provide the basis for the Team's design, development, and testing of a technology prototype that addressed one or more of the identified security exposures. Documented in the DHIAP proposal as three tasks, the work is presented in this report under a single heading because the work effort was highly integrated. The original task names and the work performed in each are:

- *Prototype Development* efforts (composed of Requirements Analysis, System Selection, Emerging Technology Research, System Design, and Prototype Evaluation efforts) –

Overview of DHIAP Phases I and II

Produce a RADIUS-compliant[25] capability for improving information security at an MTF and across the military. In addition, conduct research and develop white papers on three other ISE-identified areas of information protection where use of technology could effect broad improvement in security of the military's patient information.

- *Demonstration* efforts – Integrate the prototype technology into an MTF's operational environment, applying it to a functional healthcare system.
- *Technology Transition* efforts – Migrate the prototype technology and associated policies and procedures to operational use in the military healthcare environment.

Based on results and lessons learned in the prototype development and demonstration activities, the Team was able to recommend policies, procedures, and methodologies required to operate the demonstration system in a secure and reliable manner. The Team successfully installed, trained, and transitioned the technology to two trial site MTFs. As a result of transition activities, the military benefited from enhanced security of healthcare information at the implemented sites, and the Team was able to develop recommendations for an approach to implementing the technology across the military healthcare system.

The DHIAP prototype effort developed and proved validity and efficiency of a number of techniques for effectively identifying and implementing new technology in a complex operational environment:

- The initial activities of the RADIUS effort and the development of the emerging technology research white papers demonstrated appropriate styles of initial, or "background," research on both the technology and the target operational environment. Because of its effectiveness, this approach was later incorporated into the Phase II *General Methodology for Business Case Analysis.*
- The RADIUS effort focused on analyzing all aspects of the technology requirements and designing the solution in relation to the requirements and the needs of its intended operational environment. (For RADIUS, this meant including circumstances particular to small, community MTFs, large regional MTFs, and regional medical command technical environments.) The ensuing design and implementation plan proved, upon deployment to the demonstration sites, to be highly appropriate to and efficient for its intended environment.
- The RADIUS effort's prototyping of the technology in a lab environment prior to rollout for operational testing led to such advantages as:
  - Discovering and resolving most problems in a contained setting where they could be isolated more efficiently and operational entities were not affected;
  - Improving skills and knowledge of the development team within the controlled environment so impact on operational sites was minimized; and

[25] Remote Authentication Dial-In Service (RADIUS)

  - Allowing the prototype configurations that were to be installed in the field to be configured and tested in the controlled lab environment so they were fully, or nearly, operational when delivered to the demonstration sites.

- RADIUS final trials in the MTF and regional operational environment allowed any remaining issues to be identified and resolved, and then permitted assessment of its performance and effectiveness in the operational setting to be evaluated prior to widespread deployment. It was the demonstration site MTFs' implementation of RADIUS that formed the basis of the Phase II pre-implementation/post-implementation Business Case Analysis of RADIUS and the BCA's recommendations for future deployment by the military.

Based on the prototype implementation experience, the DHIAP Team recommended that a broad implementation of the DHIAP RADIUS-compliant technology (i.e., multi-region or command-wide) be planned and overseen by a central coordinating authority.

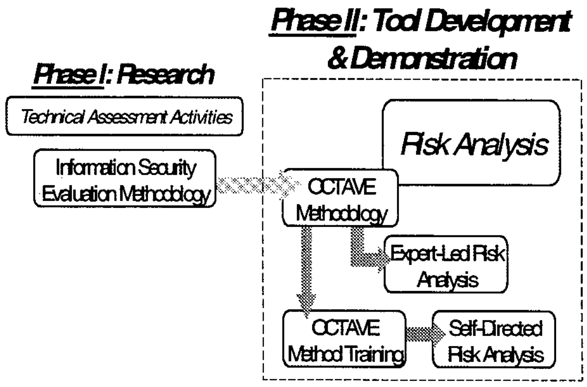
Included in this task were the investigations conducted for the Emerging Technology Research. These investigations highlight important information protection issues that may impact the MTF, but addressable primarily by higher echelons. Areas of investigation were: Remote System Administration, examining the risks of external access and administration of military health systems; Public Key Infrastructure, investigating the potential application of PKI and its impact on medical organizations; and Trust Model, analyzing intentional and unintentional trust granted to users, systems, and networks.

As indicated, the results and conclusions completed in this task pointed out the importance of conducting further research into these and related areas, and this was accomplished through activities of the Phase II Business Case Analysis Task.

DHIAP Phase II

Risk Analysis Task

Figure 8 - Overview of Risk Analysis Task


Phase II: Tool Development & Demonstration
Phase I: Research
Technical Assessment Activities
Information Security Evaluation Methodology
Risk Analysis
OCTAVE Methodology
Expert-Led Risk Analysis
OCTAVE Method Training
Self-Directed Risk Analysis

The Risk Analysis (RA) task's goal is to extend the principles of the Phase I ISE methodology to create and develop a risk assessment methodology for "self-directed" use directly by IT-dependant organizations. Building on ISE tools and techniques as depicted in Figure 8, the DHIAP Team developed an RA methodology in partnership with the Software Engineering Institute's Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) project. The methodology systematically identifies information critical assets, the elements that threaten them, and their

^{SM} Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

Overview of DHIAP Phases I and II

technical vulnerabilities. The threats and vulnerabilities are used to formulate and prioritize the information security risks associated with each critical asset. Knowing the risks, the organizations are then guided through the process of developing action plans to fix the vulnerabilities and strategies to mitigate and/or manage the remaining risks to appropriately protect the assets.

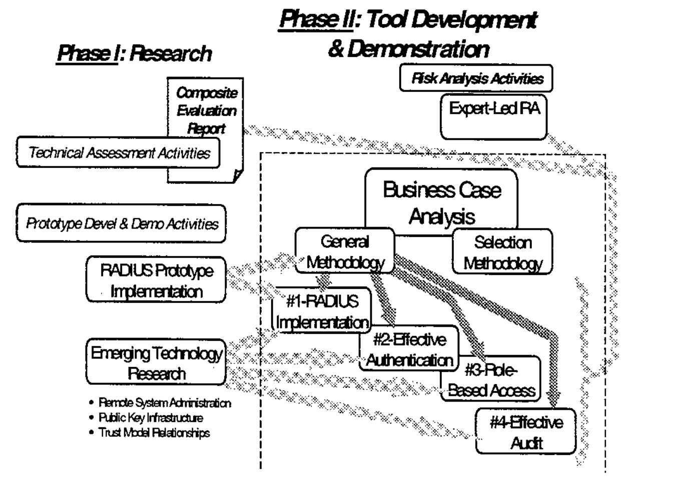
The DHIAP Team exercised the new methodology by conducting an "expert-led" RA at an Air Force MTF. After enhancing the methodology based on knowledge gained and lessons learned during those investigations, the Team refined the methodology and tools for use as a site "self-directed" tool, trained the staff of three MTFs (two Army and one Navy) on leading the study, and mentored the MTF trainees as they prepared to lead RAs at their own sites. As part of this effort, the DHIAP Team participated in TATRC's training of Medical Information Security Readiness Teams (MISRTs), presenting the purpose and an overview of the OCTAVE Method.

Based on demonstrated success of the OCTAVE method and training conducted for the self-directed teams, the *OCTAVE Method Implementation Guide* was determined to be adequate to enable MISRTs to begin their evaluations. In terms of organizational learning, it was observed that participation in OCTAVE led to immediate insights into the organizational vulnerabilities and the need for improvements on the part of analysis team members. Some sites were able to immediately apply what they learned to improve their practices.

Business Case Analysis Task

The Business Case Analysis (BCA) task was derived to address the military's need to analyze business conditions under which it should deploy technologies for promoting health information assurance in its healthcare system. The DHIAP Team began this task by drafting a methodology for conducting BCAs on subjects that might vary from information protection technologies to processes designed to protect healthcare information. The Team worked with TATRC to select subjects to be investigated using the BCA approach, focusing (as depicted in Figure 9) on subjects that had been identified as serious information vulnerabilities during Phase I ISEs.

Figure 9 - Overview of Business Case Analysis Task


Phase II: Tool Development & Demonstration
Phase I: Research
Risk Analysis Activities
Composite Evaluation Report
Expert-Led RA
Technical Assessment Activities
Business Case Analysis
Prototype Devel & Demo Activities
General Methodology
Selection Methodology
RADIUS Prototype Implementation
#1-RADIUS Implementation
#2-Effective Authentication
Emerging Technology Research
#3-Role-Based Access
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships
#4-Effective Audit

The first BCA topic selection was the Phase I RADIUS implementation. The goal of this BCA was to determine the effectiveness of the prototype and to assess costs of extending the implementation throughout the military medical system. The other topics were selected in light of both Phase I findings and the draft HIPAA regulatory requirements for user authentication, role based access, and audit of user access to patient information.

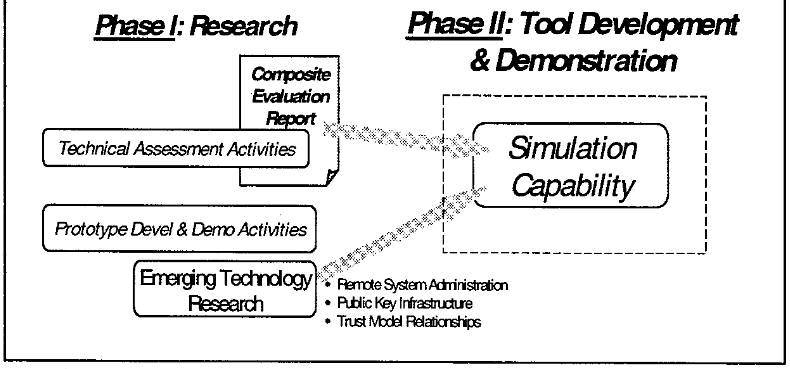
For each BCA, the Team adapted the methodology activities to be pertinent to the particular characteristics of the BCA subject and, upon conclusion of the investigation, produced a white paper documenting the purpose, background, analysis, conclusions, and recommendations of the investigation. As each BCA was completed, the team reevaluated and refined the BCA methodology based on lessons learned in conducting the previous investigation and additional activities or other components required due to the subject of the next investigation. A "general" BCA methodology emerged from this process, retaining characteristics specific to each of a number of different styles of investigation. The General Methodology for BCAs that evolved proved to be applicable to technologies and support processes across all stages of development and deployment, such as "what if" concepts, limited trial deployment, and fully operational deployments.

Recognizing the difference in perspective between some government agencies and the commercial world,[26] the Team developed the General Methodology for BCAs to be a tool to assist military decision-makers, one that considers a more comprehensive and applicable set of factors. The BCAs developed from application of this General Methodology are meant to address a wide range of issues. The BCA evaluation criteria consist of intangible, non-cost, operational, functional, and risk factors in addition to the traditional cost factors and economic analysis indicators. The result is a methodology that focuses on issues and forms of impact that are likely to be more relevant to the MEDCOM staff and/or MTF commander than just the cost of technology.

Simulation Capability Task

The Simulation Capability task called for the DHIAP Team to design and demonstrate a simulation capability that could be used to depict and analyze problems and solutions in mission survivability for military medical systems. Based on concepts developed during Phase I technology research and findings of the technical assessments at MTFs (as indicated in Figure 10), this "survivability simulator" was developed to enable stakeholders to better understand the risks and consequences of potential threats, such as cyber-based attacks to medical information systems, and potentially aid in improving and protecting the integrity, confidentiality, and availability of patient records, treatment plans, and essential medical services.

Figure 10 - Overview of Simulation Capability Task


Phase I: Research
Phase II: Tool Development & Demonstration
Composite Evaluation Report
Technical Assessment Activities
Simulation Capability
Prototype Devel & Demo Activities
Emerging Technology Research
• Remote System Administration
• Public Key Infrastructure
• Trust Model Relationships

The DHIAP Team built and demonstrated the alpha version of the survivability simulator, and drafted related supporting documentation (language reference manual and author style guides). The Easel simulation system holds promise as an effective research tool for fulfillment of critical mission requirements in infrastructures and other applications that must operate with incomplete

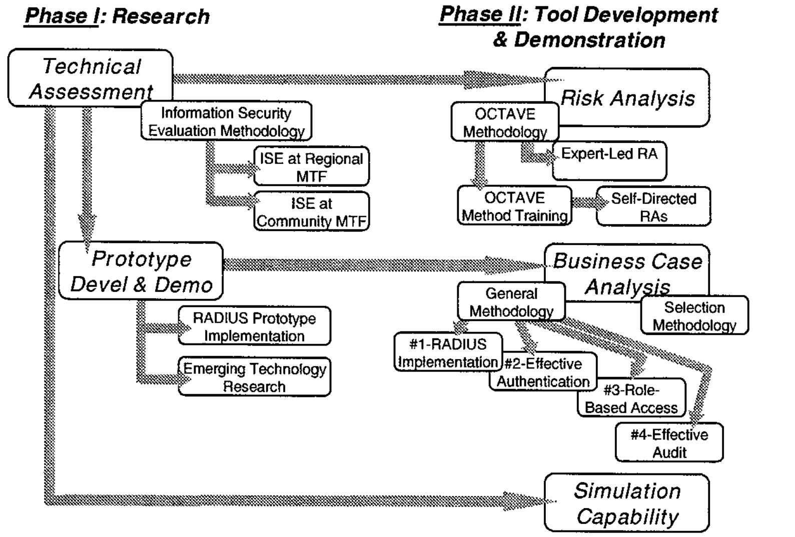
[26] Government organizations and military commanders, while keenly aware of cost issues, often assess cost more in terms of manpower requirements and impact on conduct of the operational mission. For an MTF commander, the dollar cost of a system is likely to be budgeted and covered by the system's program management office; the more important issues relate to subjects such as ease of deployment and transition, operational effectiveness, user acceptance, maintenance, security, etc.

information. Easel also overcomes several long-standing simulation barriers in terms of the accuracy of the simulation results aŋd the scalability of the models and abstractions in large-scale simulations.

DHIAP Phase I-II Conclusions

The work completed in the Phase I research and Phase II tool development, testing, and analysis program activities is summarized in Figure 11. The DHIAP Phase I and II efforts succeeded in researching the state of information assurance for military healthcare information and in developing and demonstrating in field trials new tools and techniques to allow individual organizations from MTFs to centralized authorities evaluate and manage their own facilities' state of information assurance. While the tools were developed for use in information assurance in the healthcare environment, they are adaptable and equally applicable to other areas of focus and even to other operational settings.

Figure 11 - Recap of DHIAP Phase I-II Activities and Products



Appendix 2 – MTF Support Log

Table 9 below provides a summary of MISRT queries to date (most received through the OCTAVE Information Center (OIC)). Note that all requests beginning 1 May 2003 were collected and addressed by the DHIAP Trainers as part of ongoing DHIAP support provided through the OCTAVE Training and Support (OTAS) program.

Table 9 - MTF Support Log

DATE	FACILITY NAME	RANK/NAME OF CUSTOMER	DHIAP TRAINER	QUESTION/DESCRIPTION OF PROBLEM	SOLUTION/DESCRIPTION OF SUPPORT GIVEN
5/27/2003	Naval Hospital Charleston	LTJG Saperstein	S. Pellissier	Planning workshops 2 and 3 for CNH	Established plan to assist in facilitation of workshops 2 and 3 on 10, 12, and 16 June
5/23/2003	Naval Hospital Charleston	LTJG Saperstein	S. Pellissier	Conduct of Senior Manager Workshop	Prepared for and facilitated the Senior Manager Workshop at CNH on 23 May
5/9/2003	Naval Hospital Charleston	LTJG Saperstein	S. Pellissier	Conduct of Senior Manager Workshop	Prepared and provided read-ahead material for the Senior Manager Workshop at CNH on 23 May
5/1/2003	Japan	AMEDD	J. Coleman	Discussed their OCTAVE	Discussed narrowing scope of OCTAVE (including remote clinic), time and resources required to complete an OCTAVE and initial planning for OCTAVE Kick-off; Originally trained AT has dissolved and new AT has not received training
5/1/2003	USNH Rota	LT Haytaian, Michael K.	J. Coleman	Discussed OCTAVE-S vs. OCTAVE	Assist them with the preparation of their OCTAVE; decided on choosing a hybrid using web-enabled surveys and the OAT; Helped USNH Rota prepare a planning meeting with Senior Managers, organizing the activities for various workshops and narrow the scope of their OCTAVE; Drafted Risk/Impact Evaluation Criteria and sent first draft to USNH Rota for Senior Command review and sign-off; Received Survey Responses for initial analysis and population of data in to OAT
5/1/2003	various	various	J. Coleman	Numerous requests for OIC registration	Provided tech support and help desk support regarding passwords and registration to new users
4/17/2003	Naval Hospital Charleston	LTJG Saperstein	S. Pellissier	OCTAVE process questions	Prepared for and conducted OCTAVE refresher training session for the CNH MISRT on 17 April
4/10/2003	Naval Hospital Charleston	LTJG Saperstein and CMDR Greenland	S. Pellissier	OCTAVE introduction	Prepared for and briefed Cmdr Greenland on 10 April to gain a champion on the CNH Executive Steering Committee

DATE	FACILITY NAME	RANK/NAME OF CUSTOMER	DHIAP TRAINER	QUESTION/DESCRIPTION OF PROBLEM	SOLUTION/DESCRIPTION OF SUPPORT GIVEN
4/2/2003	Naval Hospital Charleston	LTJG Saperstein and Mr. Joe Miller	S. Pellissier	OCTAVE planning and support	Met with representatives from CNH on 2 April. Plan to assist them in conducting their OCTAVE
3/11/2003	Naval Hospital Charleston	LT Holley and Mr. Joe Miller	S. Pellissier	OCTAVE at CNH	Met with representatives from CNH on 11 Mar to discuss options for supporting them in conducting their OCTAVE
2/28/2003	Naval Hospital Charleston	Joe Miller (via CIO, Bo Knight)	S. Pellissier	Request for support during the conduct of OCTAVE. They will determine needs and let us know.	We can help - awaiting requirements
1/5/2003	Navy Environmental Health Center, 620 John Paul Jones Circle, 11th floor, BLDG 215, Portsmouth, VA, 23708	Dianna Gilchrist; 757-953-0700; gilchristd@nehc.med.navy.mil	J. Coleman	Ms. Gilchrist requested an OIC account but it was unclear as to her level of OCTAVE training.	She was contacted and explained that she had received training on the initial round in 2001. She is familiar with OCTAVE. She is the MISRT lead and HIPAA POC for her facility. She is also a candidate for the next round of training.
12/6/2002	Tripler AMC	Graham Watt 808-433-4606	J. Coleman	General discussion on OCTAVE progress	OCTAVE complete. Due to deliver their final presentation to Sr. Managers that week. They completed a highly tailored OCTAVE with much of the information completed by the MISRT – "pre-processing". The MISRT consisted of 5 fully participating members. Surveys for initial workshops were distributed via email and returned successfully.
12/6/2002	78 Medical Group	Holly Ruffin 478-327-8208	J. Coleman	General discussion on OCTAVE progress	OCTAVE had reached process 2 but was currently on hold for various reasons. OCTAVE is expected to resume soon and is planned to be completed in March.
12/6/2002	Teresa Starks 805-606-9252	Vandenberg AFB	J. Coleman	General discussion on OCTAVE progress	Recently attended HIPAA training (Privacy Officer Trg?) in Denver. She is completing "Privacy 101" training for all staff in the facility before they begin OCTAVE. So far 60% of the staff have received this training. She is planning to download the OAT and will use it to help with their OCTAVE. They have 1 ½ additional staff members (SAIC) joining the team and plan to use them for OCTAVE.

MTF Support Log

DATE	FACILITY NAME	RANK/NAME OF CUSTOMER	DHIAP TRAINER	QUESTION/DESCRIPTION OF PROBLEM	SOLUTION/DESCRIPTION OF SUPPORT GIVEN
12/5/2002	Tripler AMC	Graham Watt	J. Coleman	Follow-up call initiated by J. Coleman	They are 99% complete with OCTAVE and are giving final brief to Senior Management; they found the OAT useful but it did not fit all of their data gathering practices. They had consolidated workshops during OCTAVE processes 1-3, so those sections within the OAT were not utilized.
12/5/2002	78 Medical Group, Robins AFB	Holly Ruffin	J. Coleman	Follow-up call initiated by J. Coleman	They began the OCTAVE process, but are still in early stages
12/5/2002	7 MDG, Dyess AFB	Kathy King	J. Coleman	Follow-up call initiated by J. Coleman	Their MISRT composition had completely changed except for the Team Leader; replacements for previous members not yet available. They had begun their OCTAVE with the Senior Manager's Questionnaire, but it is on-hold because of staffing issues.
12/5/2002	USCG MLCLANT	Rob Oster	J. Coleman	Follow-up call initiated by J. Coleman	MISRT had completed a scaled-down version of OCTAVE at Yorktown facility using OAT exclusively; they have plans to conduct a full-blown OCTAVE and will use the OAT as their method of data capture.
12/5/2002	Vandenburg AFB	Teresa Starks	J. Coleman	Follow-up call initiated by J. Coleman	They are 60% complete with HIPAA Privacy Training "Privacy 101." Privacy training will be completed before OCTAVE Risk Assessment activities begin.
12/4/2002	Capt. Tony Ingram	374th Medical Group	J. Coleman	Updated DSN info to commercial contact: 011-81-317755-6160	14 hour time difference made conversation difficult. Update contact information was exchanged by telephone messages.
12/4/2002	Jacob Piazana	BMC Sasebo	J. Coleman	Updated contact information: 011-81-6160-5535364	14 hour time difference made conversation difficult. Update contact information was exchanged.
12/4/2002	BMC Iwaknui	Robert Nelson	J. Coleman	General discussion on OCTAVE progress. Updated contact information: 011-81-6160-5535364	14 hour time difference made conversation difficult. Update contact information was exchanged. Information regarding OIC was given.
12/3/2002	7 MDG Dyess AFB	Kathy King	J. Coleman	General discussion on OCTAVE progress. Updated contact information: 915-696-5350 and Kathy.king@dyess.af.mil	Although the Senior Management Questionnaire had been completed in September, their MISRT team has dissolved and will have completely changed by June. 7 MDG is a candidate for the next round of training.

MTF Support Log

DATE	FACILITY NAME	RANK/NAME OF CUSTOMER	DHIAP TRAINER	QUESTION/DESCRIPTION OF PROBLEM	SOLUTION/DESCRIPTION OF SUPPORT GIVEN
12/3/2002	USCG MLCLANT	Robert Oster	J. Coleman	General discussion on OCTAVE progress	They have completed a mini-OCTAVE at the YORKTOWN clinic. OAT was used with great success. "The OAT worked very well for us – we will use it again". They are planning to complete a full OCTAVE at the Yorktown clinic in the near future. They plan to use the results from that OCTAVE to build a template for other USCG facilities to use.
12/2/2002	All MTFs that registered with the OIC, including OAT Beta Testers	Multiple	J. Coleman	All MTFs that had registered with the OIC were attempted to be contacted by telephone to discuss their progress with OCTAVE.	Many of the sites did not have accurate contact information: telephone numbers that were DSN numbers or were invalid. Most of the discrepancies were resolved by contacting base information and obtaining new department contact numbers. Some of the MISRT members had transferred to other positions or units and their replacements were untrained in OCTAVE.
10/16/2002	McConnell AFB	DOUGLAS R. ECKERT GS9 Health System Specialist	J. Coleman	Has assumed responsibility for OCTAVE. Was not one of the two people we sent to the training.	Discussed OIC registration procedures. Advised on tailoring options for smaller facilities. Explained DHIAP support options.
10/16/2002	Branch Medical Clinic MCAS Iwakuni Japan	James W. Mickey USN	J. Coleman	We got the OCTAVE software working. I am about to get started with an OCTAVE. But first I have to brief my clinic staff on HIPAA. Do you have any slide presentations to help me accomplish this task?	Sent 2 presentations: Lt. Col. Green's presentation from TRICARE conference (on TRICARE Website) and OCTAVE HIPAA Intro slides.
9/11/2002	Branch Medical Clinic MCAS Iwakuni Japan	Lt. James W. Mickey Family Practice Division Officer	J. Coleman	Requested OAT release date. Informed trainers that he has registered at the OIC and received a password.	Informed user that the OAT is nearing completion. It is currently being packed into an executable and prepared for distribution.
9/10/2002	Naval Hospital Bremerton	LTJG David S. Forsyth Health Informatics Officer	J. Coleman	Have set up a HIPAA committee	Currently focusing on Privacy. Request to allow committee access to OIC. Have not started OCTAVE but plan to begin in October 02.

MTF Support Log

Date	Facility Name	Rank/Name of Customer	DHIAP Trainer	Question/Description of Problem	Solution/Description of Support Given
9/10/2002	74 MDSS/SGSI (Wright-Patterson AFB)	McSparran Glen L Jr.	S. Pellissier	Received comments on OCTAVE implementation at the facility.	Comments reviewed by Trainers. Discussion on publishing on OIC as a "Lessons Learned" page.
9/6/2002	Keesler AFB MS 39534	Maj. Jeffrey R. Boris MD	J. Stinson	Received comments on OCTAVE implementation at the facility.	Comments reviewed by Trainers. Discussion on publishing on OIC as a "Lessons Learned" page.
9/5/2002	Misawa AB Japan	MSgt Ginno Antonio	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
9/4/2002	39 MDG/SGSI Incirlik AFB Turkey	Capt Michael D Hall	J. Coleman	Briefed our Executive Staffs an Introduction and are preparing to take the Next step) Request information on OAT. 2) Have been approached by companies soliciting HIPAA products - confused and request clarification	Advised on Release of OAT. Explained that the requirement to conduct a Risk Assessment will likely be part of the HIPAA Security Rule and OCTAVE meets that requirement. Detailed answer posted on OIC FAQ.
9/4/2002	U. S. Naval Hospital Guam	Edward Brinston	J. Coleman and J. Collmann	Requesting electronic copy of PowerPoint introductory slides "DoD Military Health System HIPAA.	Slid
9/2/2002	8th MDG Kunsan AB Korea	Lt Col Lorie Brosch	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
8/28/2002	92 MDG Fairchild AFB WA	Lt Col Ron Martin	J. Coleman	Request Information Regarding OAT.	Advised on Release of OAT and OIC information required to receive it.
8/27/2002	Kadena AB Okinawa Japan	Capt J Meneses	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
8/26/2002	Brooks AFB TX	Capt Brian L. Costello	J. Collmann	Request information on OAT.	Advised on Release of OAT
8/26/2002	Osan AB Korea	Capt Johanna Payne	J. Coleman	Responded to request for updated mailing	Information passed to S. Hartline to coordinate logistics.

MTF Support Log

DATE	FACILITY NAME	RANK/NAME OF CUSTOMER	DHIAP TRAINER	QUESTION/DESCRIPTION OF PROBLEM	SOLUTION/DESCRIPTION OF SUPPORT GIVEN
				address to receive OMIG.	
8/26/2002	USMC Branch Medical Clinic IWAKUNI	HM1(SW/FMF) MALONE	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
8/26/2002	USNH Oko	Lt Jimmy E. Francis	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
8/26/2002	US Naval Hospital Guam	LTJG Ed Macalanda	J. Coleman	Responded to request for updated mailing address to receive OMIG.	Information passed to S. Hartline to coordinate logistics.
8/21/2002	Tripler AMC	Ms Kathryn Auxer	J. Coleman	Request information on OAT and list of Sites who have completed OCTAVE	Advised on Release of OAT. List of Sites that have completed OCTAVE not yet available.
8/14/2002	Headquarters U.S. Naval Forces Europe	LT Jason Keltner CIO	J. Coleman	Requested Trainer participation in Regional Teleconference – to discuss support capabilities and HIPAA	Privacy Rule Agreed to participate and requested teleconference information
8/13/2002	Tripler AMC	Graham H. Watt	J. Coleman	Request information on OAT	OAT status provided
8/12/2002	Operations Department Norfolk VA	Leslie V. Parks PAHM	J. Coleman	Requested Tool status. Requested information regarding Tool cost and Licensing.	OAT status provided. Explained licensing for DoD (free) and no cost for internal use of tool.
7/3/2002	USNH Naples	Lt Doris Alvarez	J. Coleman	Received Survey results from Senior Commanders. Requested comments and confirmation of next steps	Replied by email with instruction on completing remainder of surveys and offered further help for conducting analysis
6/27/2002	USNH Naples	Lt Doris Alvarez	J. Coleman	Wanted help preparing briefing for senior commanders	Held teleconference to identify exact requirements

MTF Support Log

Date	Facility Name	Rank/Name of Customer	DHIAP Trainer	Question/Description of Problem	Solution/Description of Support Given
3/26/2002	Keesler AFB	Capt. Simona Allen	S. West	Wanted to know how much it would cost if they hired an outside agency to go to the Keesler Medical Center and conduct OCTAVE Training / how much money did they save by completing the task themselves?	
12/13/2001	Tripler Army Medical Center	Capt. Michelle Greene	S. West	Request for new OCTAVE CD	Sent new CD
12/13/2001	Keesler AFB	Major Jeffrey Boris	S. West	Request for new OCTAVE CD	Sent new CD
12/13/2001	HQ USAF/FG	Major Steve Greentree	S. West	Request for new OCTAVE CD	Sent new CD
12/13/2001	Eisenhower AMC	Rose Reedy BSN RN Informatics Nurse Consultant	S. West	Request for new OCTAVE CD	Sent new CD
12/13/2001		Sherry McKenzie	S. West	Communicating that CMS was expecting the HIPAA Security Rule to be final in March 02; wanted to know if this will affect plans for OCTAVE Training to begin on Feb. 02	7/24/02: no action yet; rule is still not final
11/16/2001	Keesler AFB	Major Jeffrey Boris	S. West	Wanted to know which vulnerability tools should they be using to stay in accordance with OCTAVE	Provided website name for Major Boris to download ISS; provided contact information for AFNOC CITS for a full user license key; provided contact name and number for the AFCERT; provided OIC website address for additional reference

Appendix 3 – OCTAVE-Trained Staff Who Have Enrolled for OIC Access

Table 10 below is an alphabetical listing of all OCTAVE-trained staff who requested user Ids for the OIC during DHIAP Phase III. Note that requests beginning 1 May 2003 were addressed by the DHIAP Trainers as part of ongoing DHIAP support provided through the OCTAVE Training and Support (OTAS) program.

Table 10 - OCTAVE-Trained Staff Who Have Enrolled for OIC Access

LAST NAME	FIRST NAME	TITLE	CONTACT PHONE NUMBER (IF GIVEN)	2ND CONTACT NUMBER (IF GIVEN)	EMAIL ADDRESS	TYPE OF USER
Adlesperger	Kent		907-580-6604		kent.adlesperger@elmendorf.af.mil	OIC Trained User
Alaoui	Adil		202-687-9108		alaoui@georgetown.edu	OIC Trained User
Alvarez	Maria		081-811-6358		dalvarez@naples.med.navy.mil	
Amaral	Steven		530-634-4835		steven.amaral@beale.af.mil	OIC Trained User
Angiel	Cynthia		307-773-5665		cynthia.angiel@warren.af.mil	OIC Trained User
Bert	Aaron		520-228-2631		aaron.bert@dm.af.mil	OIC Trained User
Boris	Jeffrey		228-377-6808		jeffrey.boris@keesler.af.mil	OIC Trained User
Burke	Maria		303-400-5926		maria.burke@cobuck.ang.af.mil	OIC Trained User
Cota	Scott		011-53-997-2081		sacota@gtmo.med.navy.mil	OIC Trained User
Curee	Rob		573-596-1489		Robert.Curee@us.army.mil	OIC Trained User
Curley	Benton		301-295-5628		bbcurley@bethesda.med.navy.mil	
Daniels	John		937-904-5019	937-656-7520	john.daniels@wpafb.af.mil	OIC Trained User
Davis	Gloria		270-798-8959	270-798-8962	Gloria.Davis@se.amedd.army.mil	OIC Trained User
Edward	Lane		202-782-0113		Edward.Lane@na.amedd.army.mil	
Flaherty	Patrick		360-475-4488		flahertyp@pnw.med.navy.mil	

OCTAVE-Trained Staff Who Have Enrolled for OIC Access

LAST NAME	FIRST NAME	TITLE	CONTACT PHONE NUMBER (IF GIVEN)	2ND CONTACT NUMBER (IF GIVEN)	EMAIL ADDRESS	TYPE OF USER
Forsyth	David		360-475-4945	360-475-4547	forsythd@pnw.med.navy.mil	OIC Trained User
Foster	Charles				cdfoster@sig.med.navy.mil	OIC Trained User
Francis	Sean		253-982-9139		sean.francis@mcchord.af.mil	OIC Trained User
Gilchrist	Dianna		530-634-4835		gilchristd@nehc.med.navy.mil	OIC Trained User
Giramur	Denguchi		671-366-4738		denny.giramur@andersen.af.mil	OIC Trained User
Glynn	Gary		913-684-6440		gary.glynn@cen.amedd.army.mil	OIC Trained User
Gonzales	Dominic		301-295-4634		gonzalesdv@nnd10.med.navy.mil	OIC Trained User
Haytaian	Michael		011-34-956-823673		mkhaytaian@rota.med.navy.mil	OIC Trained User
Helwig	Kent		907-580-3006	907-580-3150	kent.helwig@elmendorf.af.mil	OIC Trained User
Hornung	Kenneth		502-624-0283		hornung@amedd.army.mil	OIC Trained User
Horton	Catherine		904-542-7200 x8725		cahorton@hsojax.med.navy.mil	
Ingram	Tony		DSN 225-6160	DSN 225-8865	anthony.ingram@yokota.af.mil	OIC Trained User
Kapheim	Jennifer		303-677-3164		jennifer.kapheim@cobuck.ang.af.mil	OIC Trained User
King	Kathy		915-696-5350	915-696-5407	kathy.king@dyess.af.mil	OIC Trained User
Lawlor	Maurice		919-722-0964		maurice.lawlor@seymourjohnson.af.mil	
Mansapit	Jerri		671-344-9716	671-344-9349	jmansapit@gam10.med.navy.mil	OIC Trained User

OCTAVE-Trained Staff Who Have Enrolled for OIC Access

LAST NAME	FIRST NAME	TITLE	CONTACT PHONE NUMBER (IF GIVEN)	2ND CONTACT NUMBER (IF GIVEN)	EMAIL ADDRESS	TYPE OF USER
McSparran	Glen		937-257-6535	937-257-0342	glen.mcsparran@wpafb.af.mil	OIC Trained User
Meneses	Joey				joey.meneses@kadena.af.mil	OIC Trained User
Meyer	Felix		910-482-4057		alvin.meyer@na.amedd.army.mil	
Mickey	James		011-81-6117-53-6273		mickeyj@nhyoko.med.navy.mil	OIC Trained User
Miller	Joseph		843-743-7237		jmiller@charleston.med.navy.mil	OIC Trained User
Morales	Thomas		301-677-8865		thomas.morales@na.amedd.army.mil	
Nelson	Robert	Webmaster	253-5364		nelsonrr@nhyoko.med.navy.mil	OIC Trained User
Oster	Rob		757-628-4375		roster@mlca.uscg.mil	OIC Trained User
Parks	Leslie		757-314-6044	757-314-6481	leslie.parks@mh.tma.med.navy.mil	OIC Trained User
Pizana	Jacob		DSN 315-252-2590		pizanaj@nhyoko.med.navy.mil	OIC Trained User
Poulin	Donna		011-81-611-743-7462		poulindm@oki10.med.navy.mil	OIC User
Reedy	Rose		706-787-3568		rose.reedy@se.amedd.army.mil	
Ruffin	Holly				holly.ruffin@robins.af.mil	OIC Trained User
Sanchez	Jennifer		502-624-9968		Jennifer.Sanchez@na.amedd.army.mil	
Sandoval	Edith		757-764-8592		edith.sandoval@langley.af.mil	
Shaw	Daniel		304-876-1127		dshaw@mediadesign.com	OIC Trained User by JS
Siegworth	Gina		011-81-611-743-7594		siegworthgm@oki10.med.navy.mil	OIC Trained User
Starks	Teresa		805-606-9252		teresa.starks@vandenberg.af.mil	OIC Trained User

OCTAVE-Trained Staff Who Have Enrolled for OIC Access

LAST NAME	FIRST NAME	TITLE	CONTACT PHONE NUMBER (IF GIVEN)	2ND CONTACT NUMBER (IF GIVEN)	EMAIL ADDRESS	TYPE OF USER
Turner	Sandra	Naval Hospital Lemoore	559-998-4422	559-998-2875	sturner@nhlem.med.navy.mil	OIC Trained User
Walls	Levi		822-7916-3505	822-7916-9906	Levi.Walls@kor.amedd.army.mil	OIC Trained User
Watt	Graham		808-433-4606	808-433-1400	graham.watt@haw.tamc.amedd.army.mil	OIC Trained User
Weber	John		573-596-0131 x69325	573-596-1684	john.weber@amedd.army.mil	OIC Trained User
Wickes	Leigh		011-81-611-743-7854	011-81-611-743-7867	wickeslm@oki10.med.navy.mil	OIC Trained User
Windham	Hailey		706-544-1557		hailey.windham@se.amedd.army.mil	OIC Trained User
Woodson	Byron		315-736-4001 DSN		byron.woodson@kor.amedd.army.mil	OIC Trained User

Appendix 4 – DHIAP Phase III Technical Development Plan

Contract No. DAMD17-01-C-0048

Defense Healthcare Information Assurance Program (DHIAP)

DHIAP Phase III Technical Development Plan

Baseline

October 2001

Prepared for:
U.S. Army Medical Research and Materiel Command
Fort Detrick
Frederick, Maryland 21702-5012

This work is supported by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD 17-01-C-0048. The views, opinions and/or findings contained in this report are those of the authors and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

Change Log

for

DHIAP Phase III Technical Development Plan

The list below provides a history of changes made to the Technical Development Plan.

DOCUMENT		*CONTEXT OF CHANGE*	
VERSION	PAGE(S)	DESCRIPTION	DATE
BASIS OF REVISION:			

DHIAP Phase III Technical Development Plan

Table of Contents

Table of Figures

Table of Tables

PROGRAM DESCRIPTION

The Defense Healthcare Information Assurance Program (DHIAP) Phase III will migrate the results of the research and development efforts of the first two Phases of DHIAP to operational use throughout DOD.

Organization of Technical Development Plan

This Technical Development Plan is organized into five (5) sections. Following an overview of the Technical Management effort, it summarizes the four technical projects of Phase III. The description of each project includes the following elements:

- Brief statement of the **Purpose** of the project;
- Identification of the project's **Lead Organization** and primary **Participants**;
- **Background** description outlining the context of the effort;
- List of the **Major Activities** to be performed during the project, numbered to correspond to the project Schedule, with a narrative description of the project's tasks and subtasks;
- Itemization of **Issues and Dependencies** identified to date that might affect the Team's ability to successfully complete the activities;
- List of the **Deliverables** that will be produced by the project;
- **Schedule** for the project that indicates the participants and estimated timeframes of the major activities;
- Description of the **Travel** planned for the project, supported by a table indicating an estimate of each trip's approximate timeframe, destination, reason, and travelers (including an indication of potential travel for TATRC team members to support their planning);
- Description of **Equipment** that will or may be required to support the project; and
- Overview of **Participant Roles** and responsibilities in the project.

Appendix A to the TDP provides a Gantt chart depicting the detailed schedule for all Phase III projects.

DHIAP Phase III Technical Development Plan

1 Technical Management

DHIAP Phase III consists of four technical projects, each interdependent in some ways with the others. Managing the work includes activities such as coordinating with senior members of the project teams to plan tasks, schedules, and budgets, monitoring project progress, managing project resources, providing reporting of the projects' and overall program's accomplishments and expenditures, and preparing command and operational level briefings as requested by the Contracting Officer's Representative (COR).

Lead Organization

ATI

Participant

ADL

Background

Phase III Technical Management efforts began with activities to plan for execution of the HIPAA Summit OCTAVE Training sessions in Washington, DC. Throughout Phase III, Technical Management will use the plan as defined in the TDP as the basis for communication among Team members and for monitoring the program's progress, deliverables, resource utilization, and expenditures. Also throughout Phase III, Technical Management will provide the COR with quarterly, annual, and final reports as specified in the award documentation.

Major Activities

1.1 Initiate Phase III Work

1.1.1 Arrange to Support HIPAA Summit

Technical Management worked with the COR and the COR's technical representative to coordinate DHIAP Team efforts to prepare for and participate in the TMA HIPAA Summit's OCTAVE Training in Washington, DC, September 5-7, 2001. They arranged for ATI and TATRC staff who would conduct OCTAVE training at the Summit to receive appropriate train-the-trainer support from the SEI authors and worked with TATRC to organize the plans and staffing for conducting the Summit's four concurrent OCTAVE MISRT training courses. In addition, they identified the Team members who would provide materials needed for training (e.g., OCTAVE manuals and electronic version on CD, posters, etc.) and arranged for on-time delivery to the Summit.

1.1.2 Develop Phase III Technical Development Plan

Technical Management will prepare the DHIAP Phase III Technical Development Plan (TDP) and its associated Work Breakdown Structure (WBS). Included in the TDP definition of each Phase III project will be: identification of the responsible organization, a list of other organization(s) also participating in the project, a list of the major work activities of the project each with a description of how it will be conducted, a description of any project issues and external dependencies that are known at the time, a list of project deliverables, a schedule for conducting the work, a description and itemization of the project's projected travel requirements (with approximate timeframe, destination, reason, and travelers), a list of equipment resources required, and a brief description of the role(s) that each participating organization will play in conducting the work.

Technical Management will conduct reviews of draft versions and revisions of the TDP with TATRC as appropriate, and maintain the document.

1.2 Manage DHIAP Activities

1.2.1 Manage DHIAP Technical Work

Technical Management will oversee the execution of all DHIAP Phase III work, monitoring project execution against TDP commitments for budget, schedule, and technical goals, and monitoring changes in the project risk environment, throughout Phase III. They will evaluate the progress of the project work efforts, production of deliverables, and use of resources; if there are variances from the plan, they will work with project team members and the COR to define and execute corrective actions.

As part of overseeing project execution, Technical Management will make the necessary travel and site arrangements for the meetings and reviews defined in individual projects' work plans. Where possible, they will try to minimize travel overall by scheduling subjects of multiple projects that involve the same people into a single meeting and/or by having some meetings held as an extension to another scheduled event such as an Internal Program Review.

If Technical Management and DHIAP Team members determine that it is appropriate to change the work commitments described in the TDP, Technical Management will investigate and evaluate the basis for requesting the change. If the change is deemed necessary, Technical Management will report and justify the change to the COR and the COR's technical staff. Upon attaining the COR's concurrence on the type of adjustment to be made, Technical Management will issue a revised version of the TDP that incorporates the change into the Phase III plan of work, budgets, and schedules.

1.2.2 Facilitate Project and Cross-Project Activities

Throughout Phase III, Technical Management will oversee and coordinate activities of the individual project teams and facilitate collaboration among members of the distributed teams. This includes providing support as appropriate for electronic file transfer, electronic mail, software installation and use, and other forms of technical assistance. Technical Management is responsible for delivery of data and reports to TATRC, the COR, and the COR's technical staff.

1.2.3 Provide Regular Project Reporting

Throughout Phase III, Technical Management will collect from DHIAP Team participants the documentation that is needed to support development of the reports required by the contract. Technical Management will develop and submit the reports described in the following paragraphs:

DHIAP Phase III Technical Development Plan

1.2.3.1 Periodic Invoice and Summary of Work Performed

Technical Management will prepare invoices according to specifications Sections G and I of the contract, as well as a summary of work performed during the billing period. The invoice and work summary will be submitted to USAMRAA.

1.2.3.2 Quarterly Reports and Trip Reports

Technical Management will prepare a Quarterly Report for each three-month period that begins on 14 September 2001, and will deliver the report to the COR (4 copies) and USAMRAA (1 copy) within fifteen (15) days after the end of each quarter for all three month periods of the contract. The report will comply with the Army's formatting requirements by providing the following information:

- Technical Progress;
- Work to Date;
- Current staff with hours spent per task for the quarter and cumulative;
- Consultants with hours spent per task for the quarter and cumulative; and
- Trip Reports.

1.2.3.3 DHIAP Phase III Annual and Final Reports

Technical Management will develop an Annual Report of DHIAP Phase III accomplishments during the year that ends 14 September 2002 (the anniversary of the Phase III contract), formatted to comply with the Army's reporting requirements, and deliver it to the COR. Technical Management will also develop a Final Report at the end of Phase III that details accomplishments and lessons learned over the life of the project and deliver it to the COR.

1.2.4 Conduct Interim Program Reviews (IPRs)

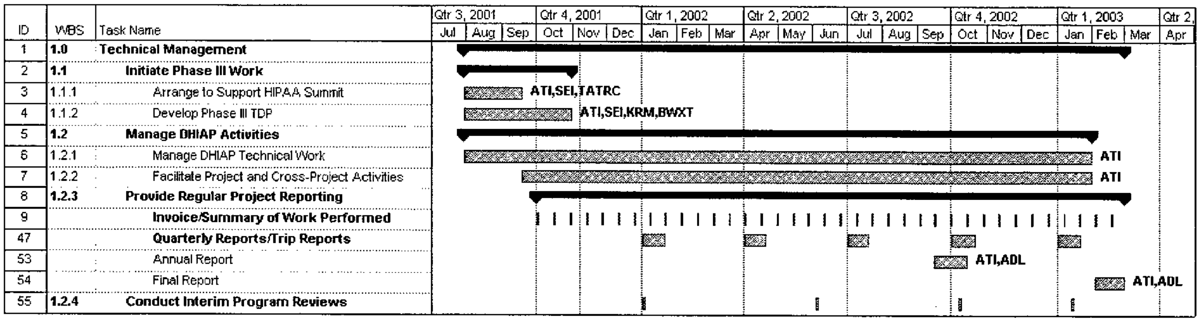
Technical Management will arrange for the DHIAP Team to conduct Interim Program Reviews (IPRs) at appropriate times during Phase III to assess progress, coordinate joint activities, revise plans as necessary, etc. The timing of these meetings will be planned to coincide with the opportunity to provide input to the COR and the COR's technical staff on work accomplished, cost, schedule, resources, quality, customer satisfaction, subcontractor relationships, and risks.

The time and place of the meeting will be coordinated with the COR. For planning purposes, tentative dates and locations of these meetings are currently identified as: the first in Charleston SC in January 2002, the second the Washington DC area in June 2002, the third in Charleston SC in October 2002, and a fourth, if needed, in the Washington DC area in January 2003.

DHIAP Phase III Technical Development Plan

Schedule

Figure 1 below indicates the activities, planned timeframes, and participants of the major activities of the Technical Management effort, as well as the high-level activities of the four technical projects.



ID	WBS	Task Name
1	1.0	Technical Management
2	1.1	Initiate Phase III Work
3	1.1.1	Arrange to Support HIPAA Summit
4	1.1.2	Develop Phase III TDP
5	1.2	Manage DHIAP Activities
6	1.2.1	Manage DHIAP Technical Work
7	1.2.2	Facilitate Project and Cross-Project Activities
8	1.2.3	Provide Regular Project Reporting
9		Invoice/Summary of Work Performed
47		Quarterly Reports/Trip Reports
53		Annual Report
54		Final Report
55	1.2.4	Conduct Interim Program Reviews

Figure 1 – Schedule for Technical Management Effort

Issues / Dependencies

- Schedules may be impacted by availability of external resources and agents. For instance, training schedules for MISRTs are dependent on hosting agents, service support, and MTF schedules. Delays in scheduled executions may impact other activities due to availability of DHIAP resources.

Deliverables

- Detailed Technical Development Plan and WBS
- Periodic Invoices and associated Summary of Work Performed Reports
- Quarterly Reports and, as required, IPR on project status and accomplishments
- Trip Reports, with electronic copies of briefings or papers related to the event
- Annual Report detailing accomplishments in the first year of Phase III
- Final Report detailing accomplishments and lessons learned over the life of the program

Travel

Travel required to support Technical Management responsibilities is summarized in the following list. Table 1 at the end of the list provides additional information about the participating organizations and number of travelers for each event.

- Initiate DHIAP Phase II Work/Arrange for OCTAVE Training at TMA HIPAA Summit:
    - ATI Technical Management staff visited TATRC in Arlington VA on August 2, 2001, to plan support for the TMA HIPAA Summit
    - ATI and TATRC staff visited SEI in Pittsburgh PA on August 21-23, 2001, to learn to train MISRTs in use of OCTAVE
    - ATI and SEI staff visited Washington DC on September 4-7, 2001, to participate in the TMA HIPAA Summit 2001.

DHIAP Phase III Technical Development Plan

- Phase III Kickoff Meeting/TDP Planning: The Phase III DHIAP Team and TATRC visited Charleston SC on October 15-16, 2001, to plan for Phase III activities and draft the Phase III Technical Development Plan.
- Interim Program Reviews (IPRs): Technical Management will plan, organize, and lead IPRs. For planning purposes, tentative dates and locations include: Charleston SC in January 2002, Washington DC area in June 2002, Charleston SC in October 2002, and, if needed, Washington DC area in January 2003.
- TATRC Meetings: As needed, appropriate Technical Management and DHIAP Team Members will conduct or attend meetings with TATRC for program communications such as obtaining guidance from and/or to present to military groups brought together by TATRC in the Washington DC area. These meetings will be arranged by the COR and the COR's representative.
- As DHIAP leader: Appropriate Technical Management will join DHIAP Team members in various meetings defined in the Work Activities for the Phase III projects.
- To publicize DHIAP efforts, compare DHIAP activity with other advanced research efforts, and gain knowledge relevant to DHIAP initiatives: The DHIAP PI and/or appropriate ATI staff will attend selected professional conferences such as the following:
    - American Telemedicine Association (ATA) 2002 annual meeting in June 2002 in Los Angeles, California

Projected travel is depicted in Table 1 below. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Table 1 - Proposed Travel for Technical Management

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
The following trips are also documented in Task 2.1, Train MISRTs in OCTAVE:				
• Aug-01 M1	*Arlington, VA w/ T1*	*HIPAA Summit Planning*	*ATI, (TATRC)*	*2*
• Aug-01 M2	*Pittsburgh, PA w/ T2*	*OCTAVE Train-the-Trainer Training*	*ATI, KRM, SEI, (TATRC)*	*6*
• Sept-01 M3	*Arlington, VA w/ T3*	*TMA HIPAA Summit 2001*	*ATI, KRM, SEI, (TATRC)*	*8*
Oct-01 M4	Charleston, SC w/ O1	Phase III Kickoff/TDP Planning	ATI, KRM, SEI, BWXT, (TATRC)	4
Nov-01 M5	Washington, DC w/ T4, O2, B1	Requirements Review	ATI, SEI, KRM, (TATRC)	6
Jan-02 M6	Charleston, SC w/ T5, O4, B2	IPR #1	ATI, SEI, ADL, KRM, BWXT, (TATRC)	5

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Jun-02 M7	Washington, DC	IPR #2	ATI, SEI, ADL, KRM, BWXT, (TATRC)	4
Oct-02 M8	Charleston, SC w/ O10	IPR #3	ATI, SEI, KRM, BWXT, (TATRC)	5
Jan-03 M9	Washington, DC w/ O12	IPR #4	ATI, SEI, ADL, KRM, BWXT, (TATRC)	4
... M10	Washington, DC	Additional Meetings with TATRC	ATI	1
... M11	Various as appropriate	Team Working Meetings	ATI	2
... M12	Various as appropriate	Conferences as appropriate	ATI	1-2

Equipment

No equipment is required to complete the activities of this task.

Participant Roles

The Technical Management project will be led by ATI, augmented as required by ADL.

- **ATI** will provide a Senior Researcher and PI to perform Technical Management tasks including: overall coordination, scheduling, and monitoring of Phase III activities; reporting and presentation of status and accomplishments; and writing, final editing, and submission of program deliverables. ATI Technical Staff (i.e., Senior Researcher, Systems Analyst, and/or Researcher) will provide collaboration support for the DHIAP Team, including electronic file transfer, electronic mail, software installation and use, and other forms of technical assistance.

- **ADL** will provide program management and monitoring expertise to support: program planning; scheduling of activities and milestones; forecasting and making recommendations on funding and funding changes; preparation for and execution of program reviews; assistance in daily tasks (e.g., resource tracking, action item monitoring, program status reporting, and preparation of deliverables); and preparation of the Monthly Invoices and associated Work Summary Reports, Quarterly Reports, Annual Report, and Final Report.

2 Deploy OCTAVE

(Requirements 1.3 and 1.2)

This task consists of two major subtasks: Train MISRTs in OCTAVE and Support OCTAVE execution. The OCTAVE training consists of a number of discrete tasks, some of which have already been executed. Close collaboration between the DHIAP Team, TATRC and the services will be required to identify and expedite decisions that will greatly affect our ability to execute the OCTAVE Training. The Support effort also consists of a number of tasks, but these tasks are interdependent and their outcomes will influence deliverables across the broad range of activities in the other Phase III OCTAVE efforts. The next two subsections discuss DEPLOY OCTAVE subtasks in detail.

2.1 Train MISRTs on OCTAVE (Mobilization)

(Requirement 1.3)

Acceptance and wide use of the OCTAVE Method and, by extension, effective integration of risk analysis into information assurance management at DOD medical centers requires training appropriate medical center staff in the use of OCTAVE and providing effective support for their execution of OCTAVE. The requirement is for the DHIAP Trainers (TATRC and ATI) to travel to regional centers and provide training to MTF MISRTs.

Lead Organization

ATI

Participants

KRM Associates, SEI, (TATRC)

Background

OCTAVE training within the DOD medical health system began when Medical Information Security Readiness Teams (MISRTs) from the DOD's sixteen largest medical centers were trained on OCTAVE at the DOD HIPAA Summit in Washington DC on 5-7 September 2001. The next stage in the rollout of OCTAVE is to train MISRTs from all remaining DOD Medical Treatment Facilities (MTFs) that have information security management responsibilities.

Major Activities

2.1.1 Develop OCTAVE Training for DOD HIPAA Summit

The DHIAP Team developed lesson plans, the OCTAVE Implementation Guide (paper and electronic) and other materials necessary for delivery of OCTAVE training. To prepare for conducting training, DHIAP Technical Management participated in a preliminary planning meeting with TATRC, and then Team members who would conduct training at the HIPAA Summit (TATRC, ATI, and KRM) met with SEI to agree on a uniform approach to training for the MISRTs. The DHIAP Trainers studied the OCTAVE Method and developed detailed scripts for conducting each course segment of the Summit, and then met on the day preceding the HIPAA Summit to confirm details of the training approach.

2.1.2 Deliver OCTAVE User Training at DOD HIPAA Summit (Initial Mobilization)

At the HIPAA Summit in Washington DC on 5-7 September 2001, following a one-day DOD overview of HIPAA for its invited DOD attendees, the DHIAP Trainers delivered OCTAVE User Training to 16 Regional MISRTs and selected other individuals designated by the DOD. The training was delivered as four concurrent seminars that lasted about 1 ½ days, followed by a brief plenary session to exchange ideas and concerns.

2.1.3 Support Wide Deployment of OCTAVE (Mobilization Training for MISRTs)

The DHIAP Team will work closely with TATRC to develop a Deployment Plan for delivery of OCTAVE training to MISRTs at MTFs throughout DOD. Major steps of the activity include the following:

2.1.3.1 **Develop Deployment Plan and Schedule**

The DHIAP Team will complete all planning for short-term deployment of OCTAVE training throughout DOD. Major activities to develop the Deployment Plan include:

- *Identify Sites*: TATRC will obtain and refine list of MTFs that are to participate in OCTAVE Training

- *Draft Schedule*: TATRC and ATI will draft an execution plan for the regional deployment (mobilization) of OCTAVE. The draft plan will take into consideration the geographical/regional distribution of MTFs designated to attend training, availability of DHIAP Trainers, conflicts with key conferences/events (e.g. HIMSS).

- *Obtain Endorsement on Execution Plan*: TATRC will submit the draft Deployment Plan to TMA and/or Service HIPAA POCs as appropriate and obtain feedback, and the Team will modify the draft plan as needed.

- *Seek Official Designation of Training Attendance*: TATRC will work with the government's authorized agent (e.g., TMA or service lead) to assure that all designated MTFs are given official communication of their designation and a request that the MTFs assign MISRT members and prepare to attend training. (This will allow the MTFs time to plan for attendance at an OCTAVE training seminar within their TRICARE Region and select appropriate MISRT members accordingly.)

- *Initiate and Oversee Training Logistics:* TATRC will work with appropriate Service contacts to assure that appropriate training sites are reserved, MISRTs are enrolled, and student travel/accommodations are arranged for each seminar.

2.1.3.2 Deliver User Training to Designated MTFs

Execution of the Deployment Plan developed in the previous task involves the following activities:

DHIAP Phase III Technical Development Plan

- *Designate DHIAP Trainers:* DHIAP Trainers will be divided into three teams of two people, each team comprised of one trainer from ATI and the other from TATRC. Team assignments will assure that each grouping contains one technically focused trainer and one process focused trainer. If a core trainer should become unavailable, the training team will be augmented by cross-assignment of experienced trainers.

- *Develop Trainer Support Package*: The DHIAP Trainers will develop the materials necessary to conduct the User Training defined in the Deployment Plan. The training material will be based on version 2.0 of OCTAVE and will include the OCTAVE Implementation Guide (IG) with trainer support to include: topic units, schedule, training exercise(s), training worksheets, lesson plans, and multimedia support material. TATRC, SEI and ATI will discuss and agree on the following:
  - Package composition (binder, CD, posters, etc.)
  - Functional requirements of package (style of instructor lesson plans—e. g., IG guidance page or checklist of lesson structure for each lesson)
  - Timeline and responsibilities for preparation of trainee support package (first draft, review of first draft, and preparation and production of final deliverables).

- *Prepare to Conduct Training:* This activity occurs in two parts, preparation and oversight for timely completion:
  - The DHIAP Trainers will meet in Charleston SC for a one-day coordination meeting/implementation briefing that will cover the Deployment Plan in detail. Agenda topics will include: ensuring all trainers are aware of their responsibilities prior to and during the training; setting activity lead-time requirements; verifying travel requirements; establishing tracking and reporting requirements. The meeting will also cover any issues raised by trainers, confirm trainer availability, identify backup trainers, and distribute updates to lesson plans/instructor checklists, etc.
  - ATI will assure that development of training materials proceeds according to the agreed schedule.

- *Produce and Distribute Student Materials*: Throughout development of the Deployment Plan, ATI will be responsible for coordinating production of the student packs (containing OCTAVE Implementation Guide, worksheet handouts, OCTAVE CD, agenda, pre- and post-training survey forms, and welcome letter containing arrival instructions and items to bring—such as a network topology diagram). ATI will coordinate the distribution of student packs to designated POCs at the host locations.

- *Schedule Training Delivery:* Early estimates indicate that twenty OCTAVE training seminars will be necessary in order to train all designated MTFs on OCTAVE. Each seminar will be two days in duration and have up to eight MISRTs in attendance. Trainers' will be assigned to regions for training, based on other commitments and associated availability. The preliminary Deployment Plan will be modified as schedules and numbers become available, in particular for the following factors:

- Adjustments to schedules for distant locations (West Coast, Europe, etc.) to reduce costs by having trainers deliver multiple training seminars in those regions before returning to their base location;
- Availability of DHIAP Trainers during critical times in the execution of other tasks in the TDP; and
- Holidays, scheduling conflicts between MTFs and other commitments.

- *Deliver Training:* The DHIAP Trainers will deliver training to designated MISRTs as described in the Deployment Plan and using the training support materials developed in this task, as they become available.

2.1.4 Identify DOD Trainers (Institutionalization)

The DHIAP Team will support TATRC to identify candidate DOD organizations for assuming responsibility for future OCTAVE training. TATRC will conduct initial research toward this goal by engaging with DOD's HIPAA Tiger Team to identify who, by appointment or role, will be charged by each service with responsibility for institutionalizing training for medical cadre in HIPAA Compliance. TATRC will work with the Tiger Team to contact the appropriate training schools and develop a plan for adoption of OCTAVE training as a primary method for teaching a newly appointed HIPAA compliance designate how to prepare for a risk assessment. As appropriate, ATI will support TATRC's effort by providing presentations and/or participating in visits with these organizations.

2.1.5 Develop Train-the-Trainer Seminar/Deliver Instructor Training to DOD (Institutionalization)

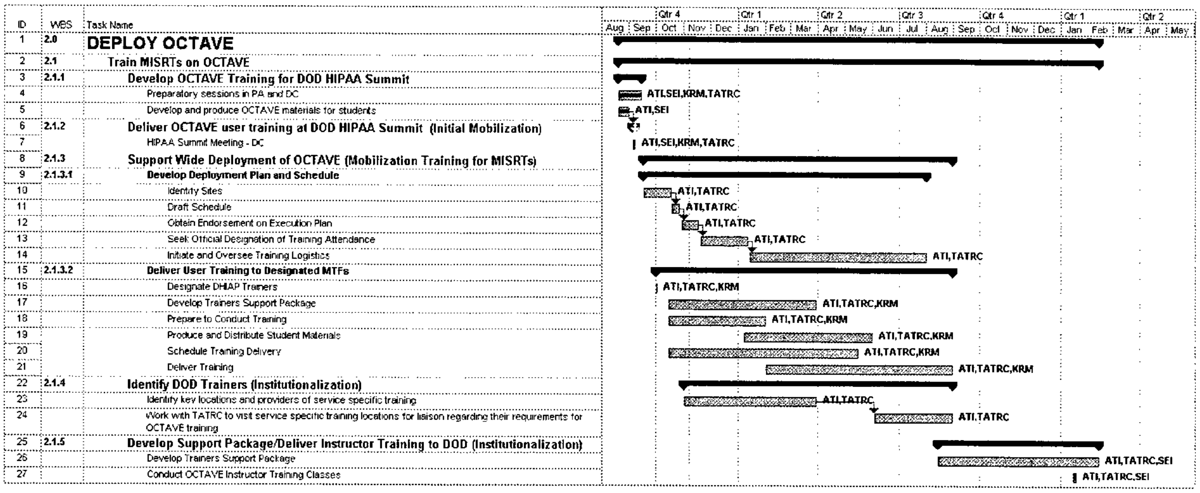
The DHIAP Team will work with TATRC to develop and execute an OCTAVE Train-the-Trainer seminar. The concept is to train trainers that will then be able to integrate OCTAVE training into the HIPAA training provided to those individuals who will assume responsibility for HIPAA compliance at their MTFs.

The Train-the-Trainer seminar will occur following completion of the initial OCTAVE User Training delivery to the regional MISRTs and initiation of those sites' OCTAVE efforts. The DHIAP Team will train the designated trainers from the services' training schools (e.g., Army, Navy, Air Force, and the Uniform Services University or other healthcare training center) on how to conduct OCTAVE training. The seminar will be focused on assisting the service training schools in development and delivery of HIPAA-oriented training, with the OCTAVE methodology as a key component for MISRT members.

Schedule

Figure 2 below indicates the activities, planned timeframes, and participants of the major activities of the Train MISRTs in OCTAVE effort.

DHIAP Phase III Technical Development Plan



ID	WBS	Task Name
1	2.0	**DEPLOY OCTAVE**
2	2.1	**Train MISRTs on OCTAVE**
3	2.1.1	**Develop OCTAVE Training for DOD HIPAA Summit**
4		Preparatory sessions in PA and DC
5		Develop and produce OCTAVE materials for students
6	2.1.2	**Deliver OCTAVE user training at DOD HIPAA Summit (Initial Mobilization)**
7		HIPAA Summit Meeting - DC
8	2.1.3	**Support Wide Deployment of OCTAVE (Mobilization Training for MISRTs)**
9	2.1.3.1	**Develop Deployment Plan and Schedule**
10		Identify Sites
11		Draft Schedule
12		Obtain Endorsement on Execution Plan
13		Seek Official Designation of Training Attendance
14		Initiate and Oversee Training Logistics
15	2.1.3.2	**Deliver User Training to Designated MTFs**
16		Designate DHIAP Trainers
17		Develop Trainers Support Package
18		Prepare to Conduct Training
19		Produce and Distribute Student Materials
20		Schedule Training Delivery
21		Deliver Training
22	2.1.4	**Identify DOD Trainers (Institutionalization)**
23		Identify key locations and providers of service specific training
24		Work with TATRC to visit service specific training locations for liaison regarding their requirements for OCTAVE training
25	2.1.5	**Develop Support Package/Deliver Instructor Training to DOD (Institutionalization)**
26		Develop Trainers Support Package
27		Conduct OCTAVE Instructor Training Classes

Figure 2 – Schedule for Train MISRTs in OCTAVE Effort

Issues / Dependencies

- Mobilization of OCTAVE: The OCTAVE Deployment Plan is contingent on identification and assembly of the MISRTs at designated training locations.
- Institutionalization of OCTAVE: The DHIAP Team's ability to complete portions of task 2.1.4 and all of 2.1.5 is dependent upon DOD's designation of organization(s) that will take responsibility for future DOD delivery of OCTAVE training.

Deliverables

- Baseline OCTAVE Method Implementation Guide (v.2.0)
- Electronic version of Baseline OCTAVE documentation
- Baseline OCTAVE Instructor's Support materials
- Baseline OCTAVE User Training materials
- Delivery of four OCTAVE User Training courses (Initial Mobilization)
- Deployment Plan for Mobilization of OCTAVE Training
- Execution of OCTAVE training according to Deployment Plan (up to twenty training seminars at various locations with up to eight MISRTs attending each)
- Train-the-Trainer seminar for Baseline OCTAVE (course)
- OCTAVE Method Implementation Guide and Trainer Support Package
- Delivery of Train-the-Trainer seminar (Institutionalization).

Travel

Projected travel required to support Train MISRTs in OCTAVE responsibilities is depicted in Table 2 below. Note that the Team Members column indicates "(TATRC)" for trips involving subjects that the TATRC team members may wish to participate in. This information is provided for TATRC's budgeting of potential travel.

Table 2 - Proposed Travel for Train MISRTs in OCTAVE

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Aug-01 T1	Arlington, VA w/ M1	HIPAA Summit Planning	ATI, (TATRC)	2
Aug-01 T2	Pittsburgh, PA w/ M2	OCTAVE Train-the-Trainer Training	ATI, KRM, SEI, (TATRC)	6
Sept-01 T3	Arlington, VA w/ M3	TMA HIPAA Summit 2001	ATI, KRM, SEI, (TATRC)	8
Nov-01 T4	Washington, DC w/ M5, O2, B1	Meeting to Develop Requirements for Trainer Support Materials	ATI, SEI, (TATRC)	5
Jan-02 T5	Charleston, SC w/ M6, O4, B2	Meeting to Prepare for Mobilization	KRM, (TATRC)	1
Feb-02 through May-02 T6	Various, TBD—see OCTAVE Deployment Plan	Travel to Conduct OCTAVE Training Mobilization (20 seminars—see Deployment Plan)	ATI, (TATRC)	Up to 2 per seminar
Sep-02 T7	TBD (Washington DC)	Conduct Train the Trainer Seminar	ATI, SEI, (TATRC)	6

Equipment

Current projections for equipment required to support the training effort are limited to the materials that will be developed for distribution to MISRTs and supplies required to conduct the training. The materials include:

- Road Map Posters
- Student copies of OCTAVE Implementation Guides and CDs
- Transparencies, flip chart paper/pens

Participant Roles

This task will be led by ATI, augmented as required by SEI and KRM Associates.

- **ATI** will provide project management, will coordinate development of the various training-related plans and development of student materials, and will participate as DHIAP trainers.
- **SEI** will provide OCTAVE subject matter expertise in general, support development of Trainer Support Materials, and will develop the OCTAVE component of the MISRT seminar training for DOD trainers.
- **KRM Associates** will participate as a DHIAP Trainer and will support development of training materials as required.

2.2 Support OCTAVE Execution

(Requirements 1.4, with elements of 1.2)

Lead Organization

ATI

Participants

KRM Associates, SEI

Background

To facilitate the transition and the broad acceptance of the OCTAVE methodology, the DHIAP Team will provide ongoing support for the execution of OCTAVE. The DHIAP Team will enroll a team of expert consultants from the Risk Database and Automated OCTAVE Tool developers (KRM and ATI), the training developers and trainers (SEI and ATI), the OCTAVE Method developers (SEI and ATI), and technical information security system experts (ATI) to provide direct, personal support for execution of OCTAVE self-directed risk assessments by DOD Medical Information Security Readiness Teams (MISRTs). The Team will coordinate the support with TATRC to ensure capabilities are developed in a manner that can be seamlessly transitioned to the DOD support infrastructure. The assistance provided to MISRTs will take various forms, but will include: direct contact with early adopters to ensure successful launch; monitoring of consultant advice to ensure adequacy and correctness; aggregation of advice in the form of "frequently asked questions" to document queries and response; and responding, as appropriate, to problem areas and road blocks to method dissemination and use. At the conclusion of the project, the DOD will have developed an effectively functioning OCTAVE support infrastructure.

Major Activities

2.2.1 Establish Support Base

The DHIAP Team will establish and coordinate a team of experts to provide direct, personal support to all OCTAVE users (MISRTs). In this support base, the first line of support for a trained MISRT will be the DHIAP Team members who trained them. These individuals will be backed up, for rapid response and resolution of issues, by subject matter experts on the various support mechanisms. As follows:

- Automated OCTAVE Tool: ATI, with support form KRM
- Risk Database: ATI, KRM, and TATRC
- Web Board Help Mechanism (includes FAQs and other content): ATI and TATRC
- OCTAVE Method: ATI and TATRC, with support from SEI
- Technical Vulnerability Analyses: ATI

2.2.2 Provide Support to MISRTs

The DHIAP Team will supplement direct, personal support with web-enabled support through RIMR. The RIMR tools developed for the central scheduling and web-board for comments and queries will be used to provide near real-time query-answer capability to the community, and will be overseen by the DHIAP Team subject matter experts for the corresponding area of concern/help inquiry.

2.2.2.1 Provide Consulting Support in Initial OCTAVE Execution

DHIAP Trainers will maintain lines of communication with MISRTs through email and telephone support, surveys and other means as appropriate for the level of progress in the OCTAVE process and type of support required by the site at that time. Initially, a short list of questions will be developed for the DHIAP trainers to use as a vehicle to establish communication with the sixteen MISRTs trained in the HIPAA Summit. The communication will also inform the MISRTs that a new version of the CD has been developed by the SEI and will be available for them to download or access through RIMR.

2.2.2.2 Develop Web Board

The DHIAP Team will establish the technical requirements for a web-board help mechanism, the OCTAVE Information Center (OIC), including requirements for a DHIAP trainers-only area that can be used for tracking site progress and sharing information between trainers during execution the Mobilization task. As part of the development, the DHIAP Team will write policies and procedures for:

- Maintaining the web-board (availability of service);
- Changing/updating content (authorization and change management/ configuration control); and
- Providing security/access control for any protected areas (e.g., trainers only area).

2.2.3 Establish and Implement Feedback Mechanisms

The DHIAP Team will develop a process for overseeing the evaluation of OCTAVE training. One approach under consideration is distribution and analysis of pre- and post-training surveys. Summarized results of help questions and answers will be furnished to the DOD along with progress tracking information as part of the Quarterly Report.

2.2.3.1 Develop Process for Overseeing Evaluation of Training

The DHIAP Team will develop a process for overseeing evaluation of training. Major activities of this effort will include:

- Review and revise pre-OCTAVE survey based on quality of responses from training conduct at HIPAA Summit;
- Review and revise post-OCTAVE survey based on quality of responses from training conducted at HIPAA Summit;
- Conduct analysis of completed pre and post OCTAVE surveys and provide feedback to TATRC;
- Use information from other help mechanisms (web-board, user-trainer contact) to identify trends that may point to gaps in training;

DHIAP Phase III Technical Development Plan

- Develop short surveys to be completed by MISRTs (or answers elicited from MISRTs by DHIAP trainers) at key stages of their execution of OCTAVE at their MTFs (e.g. at the end of each phase). This will allow the DHIAP Team to measure the effectiveness of different phases of the OCTAVE training, and also serve as an additional vehicle for tracking the progress of the MISRTs during their OCTAVE execution. The surveys will be coordinated with key milestones (e.g., at the end of processes 4, 6 and 8a);
- Draft survey content and pilot at one site that has already started OCTAVE; and
- Revise as necessary and convert to appropriate media (web based or other electronic format for ease of distribution and rapid response).

2.2.3.2 Track Site Status

- Primary Method for Tracking Site Status and Progress: DHIAP Trainers will maintain contact with their regionally affiliated MISRTs and will track progress on an ongoing basis. DHIAP trainers will telephone the MISRTs in their associated regions periodically, monthly during the evaluation phase, in order to offer support and inquire as to the progress of the site. Progress information will be consolidated from all sites and tracked with updates as necessary. Tracking information will be sorted by individual MTFs, Region, and Service. This information will be graphically displayed in the "DHIAP Trainers Only" section of the web board.
- Secondary Method: Ongoing Communication between TATRC and Service Representatives/Lead Agents.
- Supporting Methods: Information obtained from the other support activities will also be used to track site status (such as scheduled teleconferences and the survey forms completed at key stages of the OCTAVE process).

2.2.3.3 Provide Quarterly Feedback

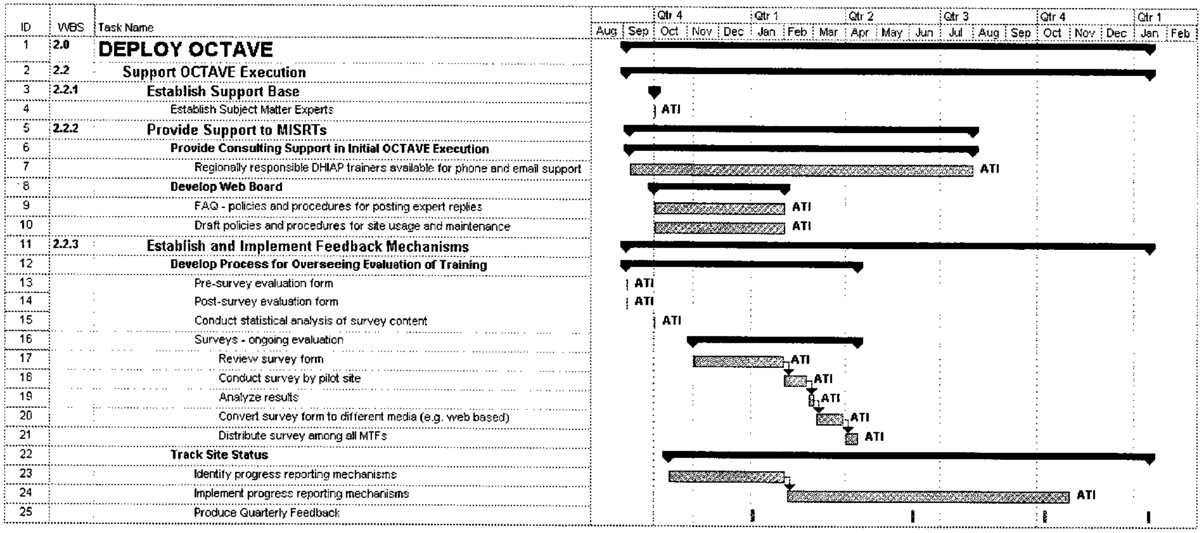
Status information will be provided to TATRC for use at the TATRC/OSD monthly meeting. Status information will also be posted on the "DHIAP Trainers Only" section of the web-board, showing progress status by region, service and individual MTFs.

In addition to the program management items, the following information will be submitted as part of the Quarterly Report to TATRC:

- Consolidated summary of help request information. (Information source will be: help requests sent to DHIAP trainers through web-board, FAQ list, regarding emails, phone calls and scheduled teleconferences).
- OCTAVE execution tracking status.
- DHIAP Team activity reports.
- Any captured recommendations for improving OCTAVE.

Schedule

Figure 3 below indicates the activities, planned timeframes, and participants of the major activities of the Support OCTAVE Execution effort.



ID	WBS	Task Name
1	2.0	**DEPLOY OCTAVE**
2	2.2	**Support OCTAVE Execution**
3	2.2.1	**Establish Support Base**
4		Establish Subject Matter Experts
5	2.2.2	**Provide Support to MISRTs**
6		**Provide Consulting Support in Initial OCTAVE Execution**
7		Regionally responsible DHIAP trainers available for phone and email support
8		**Develop Web Board**
9		FAQ - policies and procedures for posting expert replies
10		Draft policies and procedures for site usage and maintenance
11	2.2.3	**Establish and Implement Feedback Mechanisms**
12		**Develop Process for Overseeing Evaluation of Training**
13		Pre-survey evaluation form
14		Post-survey evaluation form
15		Conduct statistical analysis of survey content
16		Surveys - ongoing evaluation
17		Review survey form
18		Conduct survey by pilot site
19		Analyze results
20		Convert survey form to different media (e.g. web based)
21		Distribute survey among all MTFs
22		**Track Site Status**
23		Identify progress reporting mechanisms
24		Implement progress reporting mechanisms
25		Produce Quarterly Feedback

Figure 3 – Schedule for Support OCTAVE Execution Effort

Issues / Dependencies

- Escalation Path for MISRT Issues: Path for escalation of an issue to higher levels of support is currently undefined (e.g., the point at which a telephone support should migrate to a VTC, and then to a site visit). At present, funding is available to provide support through scheduled teleconference calls, ad-hoc phone calls, and email messages.
- Frequency of DHIAP-Originated Trainer Contact with MISRTs: The chain of events for DHIAP Trainers making contact with MISRTs and guidelines for the following activities have not yet been determined: how often a DHIAP Trainer should contact the MTF, how contact should be made (e.g., through TATRC, through Lead Agent or directly), and how the activity should be tracked and recorded.

Deliverables

- Direct pro-active contact with MISRT and consultant advice and assistance
- Web-based OCTAVE collaboration facility, with procedures for MISRT submission of questions
- Problem resolution support for MISRT OCTAVE questions
- Compilation of FAQs about OCTAVE execution for inclusion in RIMR
- Quarterly "Summary of OCTAVE Site Activity" report (submitted as part of the DHIAP Quarterly Report)

Travel

No travel is anticipated to complete the activities described for this task.

Equipment

No additional equipment is required to complete the activities of this task.

Participant Roles

This task will be led by ATI, augmented as appropriate by SEI and KRM Associates.

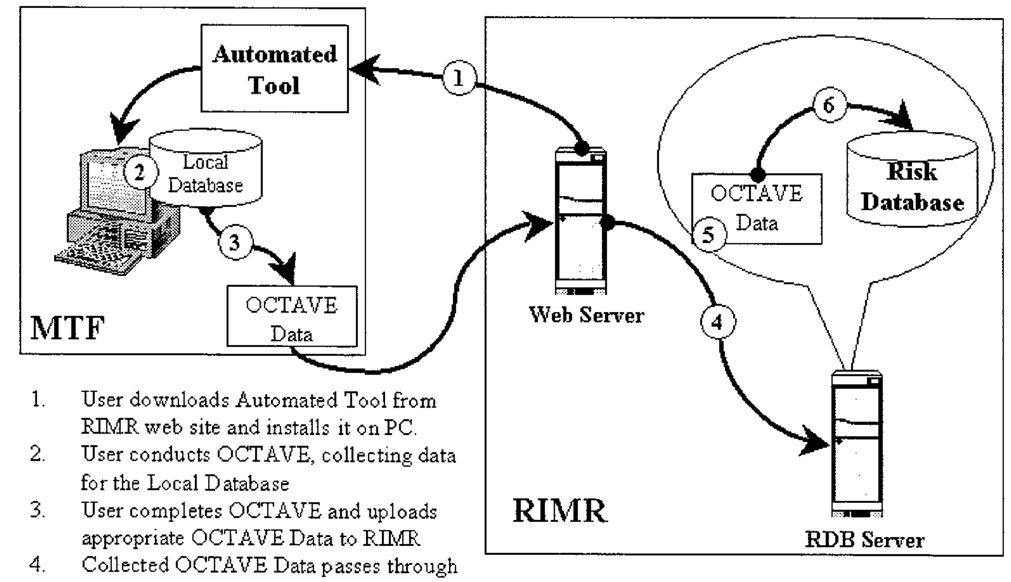
DHIAP Phase III Technical Development Plan

- **ATI** will provide project management and will be the principal provider of all support activities. ATI will provide expertise on the Automated OCTAVE Tool, Risk Database, Web Board development and technical support, and Technical Vulnerability Analyses.
- **KRM Associates** will provide expertise on the Risk Database and will serve as a backup DHIAP trainer if needed.
- **SEI** will provide expertise on the OCTAVE Method.

3 OCTAVE Tools

(Requirements 1.1 and 1.2.2)

This task consists of two major subtasks: The first is to design, develop, and provide a PC-based Automated OCTAVE Tool. The second is to design, develop, and install a Risk Database. As shown in Figure 4 below, the two tasks are mutually dependent, in that the information gathered by the Automated Tool during a site's conduct of OCTAVE feeds the Risk Database.



1. User downloads Automated Tool from RIMR web site and installs it on PC.
2. User conducts OCTAVE, collecting data for the Local Database
3. User completes OCTAVE and uploads appropriate OCTAVE Data to RIMR
4. Collected OCTAVE Data passes through RIMR web server to RDB server
5. Collected OCTAVE Data is held for evaluation/validation
6. Validated OCTAVE Data is placed in Risk Database

Illustration of how a user would download and run the Automated Tool, then upload the collected data to the Risk Database

Figure 4 – Interrelationship of Automated OCTAVE Tool, RIMR, and Risk Database

The next two sections discuss each subtask in detail.

3.1 Automated OCTAVE Tool

(Requirement 1.2.2)

This portion of the OCTAVE TOOLS effort develops and pilots a PC-based Automated OCTAVE Tool (Tool) to support site execution of the OCTAVE processes, and provides the tool to TATRC for wide distribution. The Tool will guide a site's Medical Information Security Readiness Team (MISRT)—the site's OCTAVE analysis team—through the OCTAVE process steps and support production of the necessary reports for the site's use. It will implement the information model guidelines developed for the Risk Database (RDB) for capturing data and generating essential reports. The Tool will provide a Graphical User Interface (GUI) for direct, computer-based entry of OCTAVE data (with data quality assurance checks incorporated into the

DHIAP Phase III Technical Development Plan

data collection process), retention of that data in a local data store, and an interface to the RDB, ensuring the ability to securely transfer data from the local source to a centralized database. The core functionality of the GUI will be to facilitate the OCTAVE process scribe functions by supporting the collection of OCTAVE assessment data and prompting the user through the proper sequence of the OCTAVE process steps.

Development of the Tool will use fourth generation software development tools. As necessary, documentation for installing the Tool and guidance for using it to conduct a site OCTAVE risk analysis will also be developed. The Tool will be packaged as a user-installable software product, downloadable from the RIMR. The Tool will be used locally by the MISRT for collecting local data for later upload to the central RDB. Software design and development for the Tool will occur in parallel and in close association with design and development of the RDB.

Lead Organization

ATI

Participants

KRM Associates, SEI

Background

While good security practice requires that there be ongoing attention to performing information assurance risk assessments and maintaining a Risk Management plan, the process can often be very paper-intensive and challenging to execute, and require intensive post-assessment synthesis of results. This project develops an Automated OCTAVE Tool that incorporates the features of the proven OCTAVE Method risk assessment methodology and offers the additional benefit of both guiding and supporting DOD MISRTs through the OCTAVE process. Through use of this tool, MISRTs will be capable of maintaining all information collected to support their risk assessment activity in a PC-based tool. As a result of MISRTs' use of the Tool to document their findings and conclusions, the information collected by numerous sites will be compatible across sites and may be made available (through upload to the DHIAP-developed RIMR Risk Database) for analysis and use by higher echelons, allowing identification of information vulnerabilities that may have more of a systemic (vs. site) basis for their existence.

The Tool developers will use a modified waterfall life cycle development process. The modification of the typical waterfall development process will be to maximize parallel design and development activities where possible in order to meet an aggressive development schedule.

Major Activities

The major activities in this task are outlined below. Periodic "checkpoints" to ensure the products meet Government expectations along the way will be key to operational success.

3.1.1 Specify Requirements

Primarily during October and November 2001 meetings with TATRC, the DHIAP Team assessed user requirements[27] for the Tool in order to describe the functional and technical

[27] The DHIAP team coordinated the draft requirements specifications with TATRC, obtained feedback, and adjusted as necessary.

capabilities at both the system and software levels[28] that must be present in the Tool and the supporting context for how the Tool will be integrated with the OCTAVE process. The requirements identified in this document are based upon the following fundamental requirement:

> *The scribe/facilitator will use the Tool to complete an OCTAVE. It will capture all OCTAVE data that the scribe would retain and carry forward to a future process (i.e., that information upon which group consensus has been obtained).*

3.1.1.1 System Requirements

The system requirements are described in terms of functional capabilities, technical requirements, and operational requirements. User requirements primarily influence the functional capabilities, which describe what the Tool must "do." Functional capabilities will also identify particular functional quality assurance attributes, which the tool should possess. Technical requirements focus more on what the Tool needs to operate, in terms of the computer on which the Tool is loaded and that computer's operating system. Operational requirements consist of the performance and physical characteristics and operational conditions within which the product must perform.

This section first establishes the foundation upon which the system requirements will be developed by listing a set of design assumptions. Following those assumptions are the functional capabilities, technical requirements, and operational requirements. The System Requirements section concludes with an outline of the user documentation, which includes installation and operation guidance, process flow (i.e., explaining when the Tool should be used in site execution of OCTAVE), etc., that will accompany the Tool.

3.1.1.1.1 Assumptions

- The Tool user is a member of the MISRT (OCTAVE Analysis Team)
- The Tool user has been trained in OCTAVE (Reference: OCTAVE Method Implementation Guide (OMIG), Version 2.0)
- The individual who downloads the Tool is an authorized RIMR user
- The Tool user is familiar with Windows NT/2000 and Microsoft Office
- The Tool user can obtain the privileges needed to load the Tool on the PC/workstation
- The PC/workstation upon which the Automated Tool will be loaded and used has Internet connectivity and is loaded with (minimally) Windows NT/2000, Microsoft Office 2000 with Access, and Internet Explorer 5.0 or Netscape. Note, that the PC/workstation may be a laptop, and it need not remain connected to the network for the duration of OCTAVE execution – only for download of the Tool from RIMR and upload of the data to the RDB.

[28] The "system" is the complete Automated Tool package. The "software" is the primary component of the system but refers specifically to the automation of the OCTAVE process.

- The site and/or Tool user will ensure current patches are loaded on the PC/workstation upon which the Tool is loaded
- The site and/or Tool user will enforce security protections on the PC/workstation upon which the Tool is loaded; likewise, the site will protect the data collected to the necessary level – whatever they deem that to be
- The Tool user will not change Tool versions during the conduct of the OCTAVE
- The Tool will transfer all site collected data to the RDB unless the Tool user chooses to not send selected data

3.1.1.1.2 Functional Capabilities

- Allow the Tool user to download (i.e., obtain electronically) the Tool in the form of an installation package from RIMR
  - RIMR will have a link for downloading the Tool
  - The Tool installation package will be a self-extracting .exe and/or a zipped file
    - The installation package will include User Documentation text files and a README file for getting started
- Guide the Tool user through completion of OCTAVE (via GUI), capture OCTAVE data, and produce a final report (see Software Section below for details)
  - A start screen will provide access to executing OCTAVE Processes, checking status, and gathering other relevant information (e.g., demographic site data, start/end dates, etc.)
  - Process tracking – the Tool will inform the Tool user of progress
    - Where (in the OCTAVE Processes) the user is during the conduct of OCTAVE
    - Where the user left during previous work
  - The Tool will provide a means for data quality assurance checks (see the Software Section below for details)
- Provide the Tool user with options to assist/support the process, to include: Print, Help, Edit/Review, and View Example (see Software Section below for details)
- Integrate the OCTAVE workgroup surveys
  - *Assumption*: Site MISRT distributes and collects the Senior Management, Operational Managers, Staff/IT Surveys
  - The Tool will aid in the compilation of Senior Management, Operational Managers, Staff/IT Survey results and allow the Tool user to view the survey results
  - Surveys will be tailorable at RIMR, but not at the site level
- Secure upload of local site data collected in the execution of OCTAVE to RDB
  - Default will be to upload all locally collected data to the RDB
  - As an option, the Tool user may select the data that is sent
    - Minimum upload will be the demographic data and the Final Report data

        - Selectable options will be the other logically grouped groups of data (e.g., APW(s), vulnerabilities and components scanned, workshop attendees, etc.)
    - Establish SSL connection with RIMR web server or RDB server
    - Transfer data
- Retain local data
    - Fixed (read only) copy of collected data that preserves the results of the OCTAVE so users can, at some time in the future, review un-modified OCTAVE data
    - Editable copy of collected data that the site can modify according to their needs and from which they can generate their site specific reports
- Integration of the capabilities to collect and report OCTAVE information related to HIPAA, DITSCAP, and JCAHO information (once that information has been specified by DHIAP Task 4.0)
    - Correlation to HIPAA, DITSCAP, and JCAHO information requirements
    - Ability to generate HIPAA, DITSCAP, and JCAHO related reports
- User documentation (see User Documentation subsection below for details)

3.1.1.1.3 Technical Requirements

- Interface to RIMR and RDB
    - Electronically accessible (downloadable), installable, self-extracting .exe and/or .zip file(s)
    - Upload to RDB via 128 bit SSL[29]
- Executable in the Windows NT/2000 environment
- Ability to ensure the environment (PC/workstation) will support the Automated Tool
- Fourth generation tool for development of the Automated Tool system
    - Microsoft Access should be capable of being packaged into a downloadable, installable application. With a script (like Visual Basic) it should also be capable of uploading the data to the RDB.
- Relational database (e.g., Microsoft Access) and data dictionary/schema
- Ease of installation of executable by use of tools such as DemoShield, which can be used to package the software application
- Error handling procedures will attempt to ensure graceful degradation of the Tool should a fault/error occur during operation
- Manual and automatic, periodic backup/save of data collected; this will preserve the data input to at least the last completed OCTAVE Process
    - This will allow for the restoration of data (back to the last completed Process) should the system crash

[29] Secure Sockets Layer (SSL) is a security protocol designed by Netscape Communications Corporation. SSL is designed to provide security during the transmission of data over TCP/IP. SSL provides data encryption, server authentication, and message integrity for data transmission over the Internet. SSL 2.0 supports server authentication only, while SSL 3.0 supports both client and server authentication.

  - *Assumption* – the Tool user will be capable of either moving the backed up version of the data into the current working directory or pointing the Tool to the backed up version to open it; User Documentation will provide the steps to accomplish this
- Version/configuration control reside with RIMR

3.1.1.1.4 Operational Requirements

Operational requirements consist of those organizational, operational user, maintenance, and security requirements necessary to support fulfillment of the system's objectives.

3.1.1.1.4.1 Organizational Requirements

- Most organizational requirements are similar to those conditions necessary for completion of an un-automated OCTAVE process:
  - Command sponsorship of completing the OCTAVE process
  - Interdisciplinary, trained MISRT (i.e., the OCTAVE analysis team)
  - Participation in workshops
  - Completion of Senior Management, Operational Managers, Staff, and IT Surveys
- PC/workstation that meets the minimum configuration requirements upon which to load the Tool
- Protection of the PC/workstation upon which the Tool is loaded, the Tool itself, and the data the Tool collects

3.1.1.1.4.2 Operational User Requirements

- Trained in OCTAVE, OMIG Version 2.0
- Basic knowledge of the Windows NT/2000 operating system and Microsoft Office; detailed knowledge of Office tools (e.g., Access, Word, Excel) is not necessary for Tool operation, but would facilitate the site use of collected data
- User account privileges to install software on PC or assistance in installation

3.1.1.1.4.3 Data Maintenance Requirements

- Maintenance and re-use of the site collected data will be a site responsibility; if the site desires to retain copies of collected OCTAVE data, they will need to ensure the data files are transferred to a more permanent storage location (such as a file server) so the files are not lost if the original PC/workstation is replaced/upgraded
- Current operating system and Microsoft Office updates and patches will be a site/user responsibility

3.1.1.1.4.4 Security Requirements

- Security of the data collected at the site will be the responsibility of the site
- The Tool and the data collected in the process of conducting OCTAVE will be secure to the extent that the PC/workstation upon which it is loaded and data files transferred to a permanent storage location are secured by the site

3.1.1.1.5 User Documentation

- How to prepare for conducting an OCTAVE using the Tool

  - Brief senior management
    - Gain support
    - Identify operational areas to evaluate
  - Schedule workshops
  - Distribute surveys
  - Obtain network infrastructure diagrams
- How to use the Tool
  - Getting Started
    - Finding information (e.g., explanation of font and format in user documentation)
    - Minimum PC/workstation configuration requirements (to be reviewed, and updated as necessary, upon new releases) and patch levels
    - Tool installation
    - Executing the Tool
    - Restoring Data – in the event that the system crashes during Tool execution, Tool user will be guided through the steps of restoring the data from the periodically backed up data (i.e., either moving the backed up version of the data into the current working directory or pointing the Tool to the backed up version to open it)
  - Command Reference
  - How to Obtain Help (e.g., link to OCTAVE Information Center)
  - Deviation from the OMIG
    - Description of how the Tool has been tailored
    - Explanation of terminology differences between the Tool and the OMIG (e.g., the use of "Security Values" rather than "Security Requirements")
    - Guidance on how the Tool can be tailored by a site during its conduct of OCTAVE
- Process Flow

3.1.1.2 Software Requirements

The Tool's software component supports the system. As the primary component of the system that provides the GUI that guides the user through the OCTAVE process and captures the relevant data, it warrants a detailed description of its requirements. This section describes the software's functional capabilities, its technical capabilities, and the data definition and database requirements. Functional and technical capabilities closely parallel the descriptions already provided at the system level. The database requirements will specify the data definitions (e.g., inputs/outputs, descriptions, etc.) and the schema.

3.1.1.2.1 Functional Capabilities

- Guide the user through the OCTAVE process (basically following the steps of the *OCTAVE Method Implementation Guide* (OMIG), Version 2.0)
  - Graphical, user-friendly interface

- User will navigate the OCTAVE process based on data input completion and command buttons
- User will be capable of paging through most screens to get a feel for the Tool, but data entry checks will prevent the user from inputting invalid data (e.g., the user will not be allowed to enter an area of concern without first identifying an asset)
- Tool flexibility will allow for some variations in the Process order for completing OCTAVE (e.g., should the site choose to reverse the order of Processes 1-3, allowing the senior managers to provide input to the Evaluation Criteria in Process 7); however, the Tool's primary concern will be in maintaining the integrity of the OCTAVE process, rather than flexibility
  - A capability for the Tool user to capture "Parking Lot Issues" (i.e., ideas that apply to other processes/workshops/activities) may offer a means to provide flexibility in the Tool
  - Warnings to the Tool user for inappropriate data entry or Process order will be available (but will not to the extent that they are a nuisance and/or they interfere with flexibility)

- Data collection and retention
  - Collect necessary data
    - Demographic site data
    - OCTAVE data that the scribe would collect or need to carry forward to future Processes
  - Local database will store the information collected during Tool execution
    - Relevant data will be kept current during OCTAVE execution
      - Data will be maintained and available during the execution of the OCTAVE Processes
      - Locally stored data will be saved periodically as the user navigates the Processes
    - Relevant data will be complete
      - The system will verify Process outputs have been captured
      - User prompts and directions will guide the Tool user to complete the data entry
    - Relevant data will be correct
      - Data field definitions will, to the extent possible (given the capabilities of Microsoft Access), exclude impossible values
      - Data field definitions will prompt the user to validate unlikely values (given the capabilities of Microsoft Access)
    - Relevant data will be coherent
      - Data will be entered, stored, and retrieved in an organized fashion
      - The software will assure that the data is delivered to the right data field in the database

            - Data fields will be predefined where appropriate and categorized in an analytically and administratively useful structure

- Produce output
    - Intermediate reports, such as:
        - Consolidated assets, areas of concern, and security requirements for starting Process 4
        - Evaluation Criteria table created in Process 7
        - Others, as appropriate, to complete OCTAVE (TBD)
    - Asset Profile Workbook for each critical asset
    - Survey results
    - Draft OCTAVE Final Report
    - Data for transfer to the RDB will be selectable by the Tool user
        - Default will be to upload all locally collected data to the RDB
        - Minimum upload will be the demographic data and the Final Report data
        - Selectable options will be the other groups of data (e.g., APW(s), vulnerabilities and components scanned, workshop attendees, etc.)
    - Allow the user to utilize OCTAVE information to produce reports relating to HIPAA, JCAHO, and DITSCAP, as identified in DHIAP Task 4.0 (once identified)
- User Environment Options
    - Print Options. A Print Option will allow the user to print the following:
        - Current screen
        - Worksheet(s) associated with the current OCTAVE Process
        - Data collected from a selected OCTAVE Process
        - Raw data collected, sequenced, but unformatted
        - Draft Final Report
    - Help Options. A Help Option will allow the user to obtain help in the following manners:
        - Tool Help
            - How to use the Tool
            - Explanation of progress tracker
            - Who to call for help and/or a link to the OCTAVE Information Center
        - OCTAVE Help
            - Refer to the slides for the current OCTAVE Process
            - Refer to the Guidelines for the current OCTAVE Process
            - View the worksheet(s) associated with the current OCTAVE Process
            - View the Example associated with the current OCTAVE Process
            - View the entire OCTAVE Example

    - Description of the tailoring restrictions
  - Stop work / continue capability (e.g., start a new OCTAVE and/or open an existing OCTAVE file and continue work)
  - Capability to review, edit/correct, and delete data prior to completion of OCTAVE and submission to RDB

3.1.1.2.2 Technical Requirements

- Fourth generation tool (Microsoft Access) for development of the Tool software
- Microsoft Access application
- Frequent, automatic data save actions to ensure data is not lost – at least up to the current Process
- Ensure data and user input is complete/correct (e.g., the user cannot input an area of concern if there is no asset)
- Hyperlinks will allow access to OCTAVE slides, worksheets, examples, and guidelines

3.1.1.2.3 Database Requirements

- Data definitions for data collected by the Tool will be described in the Risk Database definition
- Copies of the locally collected data will be available to the site (as described in the System Requirements)

The DHIAP Team conducted formal reviews (October and November 2001) of the requirements developed above with TATRC and the rest of the DHIAP Team and obtained and incorporated feedback on the recommendations, assumptions, and design decisions.

3.1.2 Develop System and Software Architectural Design

Coordination of system and software activities facilitates communication among the designers and other key stakeholders to clarify requirements and impacts on the design of the system. The architecture is a means for formulating and recording system and software design decisions (e.g., decisions about the software's behavioral design and decisions affecting the selection and design of software components).

Using the requirements specifications from Activity 3.1.1 and the technical criteria of the selected COTS development tools as a guide, the Team will develop a coordinated top-level design for the technical components of the Automated Tool, including, as required:

- GUI design with draft layouts of screen format to be used in the application, along with descriptors indicating special processing and/or editing requirements for input fields;
- Design for the Tool's local database (e.g., length of field, alpha vs. numeric input, range of acceptable values, etc.);
- Design for the interfaces external to the software and between the Tool's software components;
- Design for the upload interface capability to the central RDB;

- Preliminary versions of user documentation;
- Design for integration of the Tool with the OCTAVE methodology; and
- Preliminary test procedures.

Throughout the design process, the Team will coordinate Tool design decisions with the designers/developers of the RDB and other relevant stakeholders, such as SEI's OCTAVE developers, to ensure functional compatibility for uploading relevant captured data from the Tool to the RDB. Upon completion of the design, ATI will conduct a design review with TATRC and update the design, as appropriate, based on results of the meeting.

3.1.3 Perform Software Coding, Testing, and Integration

Using the tools selected and the design developed in Activity 3.1.2, ATI will develop a prototype Automated Tool consisting of the GUI, the local database, and the upload (to the RDB) capability. The effort will include acquisition of development tools. The software components will be coded and integrated using development support tools to the maximum extent possible to reduce development time. Individual software units and software components will be developed, with Alpha and Beta version releases, and tested prior to integration to ensure that each satisfies its requirements. Regression testing of aggregate components will ensure proper functionality of the whole. Included within this activity, user documentation will be updated as required.

3.1.4 Perform Software Qualification Testing

Laboratory testing will be conducted to ensure Tool capabilities are traceable to system and software requirements, external and internal operations are consistent with system requirements, and user documentation is up to date. The Team will demonstrate the prototype to TATRC and other stakeholders for evaluation and feedback.

3.1.5 Perform System Integration and Qualification Testing

Ideally, ATI will work with an experienced MISRT executing an OCTAVE at a trial site selected by TATRC to test the usability of the Automated Tool. Alternatively, if a MISRT is not available to meet the schedule, the beta version of the system will be extensively tested in the laboratory and/or other non-MTF test site. Throughout the qualification testing, the Team will gather feedback on the product's usability and technical features, and evaluate the need to make immediate field changes to the product vs. holding them to be used in the next version, or deferring them as "nice-to-have" in a post-DHIAP Phase III version.

Upon completion of the beta test, the Team will meet with TATRC to evaluate prototype functionality and capability in meeting stated requirements and to make a checkpoint decision. The Team will review the beta test feedback issues with TATRC, indicate the Team's classification of outstanding issues/changes (as necessary, nice-to-have, or rejected) along with rationale for recommendations, and then work with TATRC to identify the changes that must be included in the product version of the Tool.

3.1.6 Refine Tool and Develop the Installation Package

The DHIAP Team will refine the Tool based on the results OCTAVE Comparative Analysis effort (Task 4.0 below) and on the results of the system qualification test and analysis. They will also develop an installation package and user documentation to support user installation and operation of the Automated Tool.

The installation package will be developed as a self-contained application that users can download from RIMR and install (e.g., via a "wizard," like InstallShield). Design of data transfer between the Automated Tool and the RDB will employ industry standard secure methods for exchanging data.

The Team will work with RIMR support staff to test capabilities for downloading the installation package from RIMR. Later, when the RDB development effort is at the appropriate stage of its development and is testing RDB capabilities with RIMR, the Tool development Team will support tests that involve uploading a site's data from the Automated Tool to the RDB in the RIMR environment. Successful testing will lead to transition of downloadable tool configuration to RIMR.

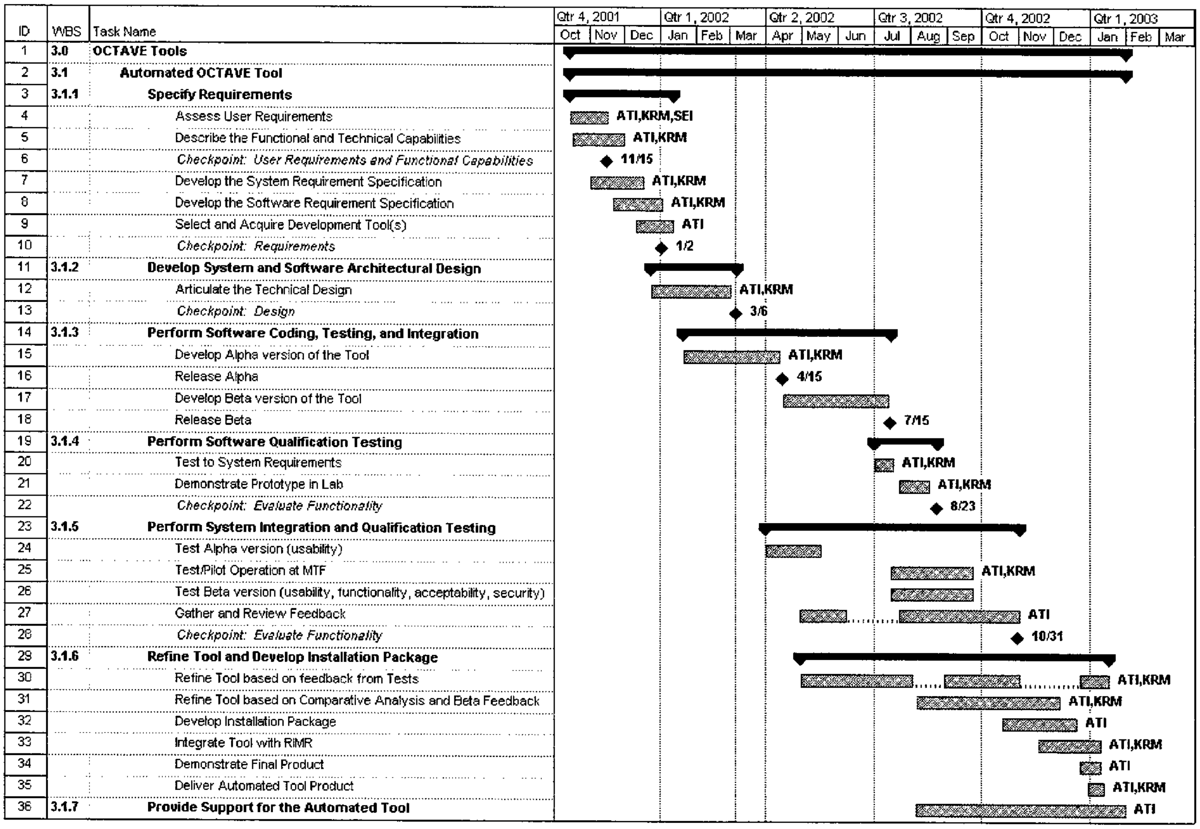
3.1.7 Provide Support for the Automated Tool

The OCTAVE Information Center (OIC) will provide the initial mechanism for MISRT reporting of problems with the automated tool, and the DHIAP Team's responses. The Tool developers will be responsible for addressing each reported problem with the Tool. Where the problem should be fixed through operational procedure, the Team will provide the material to be used in the response and capture for potential inclusion in FAQs. Where the problem relates to software/hardware issues, the most appropriate DHIAP resource (either Tool developers or OIC staff) will work with the MISRT to appropriately define the problem and to develop and implement the fix.

DHIAP Phase III Technical Development Plan

Schedule

Figure 5 below indicates the activities and planned timeframes of the major activities of the Automated OCTAVE Tool effort.



ID	WBS	Task Name
1	3.0	**OCTAVE Tools**
2	3.1	**Automated OCTAVE Tool**
3	3.1.1	**Specify Requirements**
4		Assess User Requirements
5		Describe the Functional and Technical Capabilities
6		*Checkpoint: User Requirements and Functional Capabilities*
7		Develop the System Requirement Specification
8		Develop the Software Requirement Specification
9		Select and Acquire Development Tool(s)
10		*Checkpoint: Requirements*
11	3.1.2	**Develop System and Software Architectural Design**
12		Articulate the Technical Design
13		*Checkpoint: Design*
14	3.1.3	**Perform Software Coding, Testing, and Integration**
15		Develop Alpha version of the Tool
16		Release Alpha
17		Develop Beta version of the Tool
18		Release Beta
19	3.1.4	**Perform Software Qualification Testing**
20		Test to System Requirements
21		Demonstrate Prototype in Lab
22		*Checkpoint: Evaluate Functionality*
23	3.1.5	**Perform System Integration and Qualification Testing**
24		Test Alpha version (usability)
25		Test/Pilot Operation at MTF
26		Test Beta version (usability, functionality, acceptability, security)
27		Gather and Review Feedback
28		*Checkpoint: Evaluate Functionality*
29	3.1.6	**Refine Tool and Develop Installation Package**
30		Refine Tool based on feedback from Tests
31		Refine Tool based on Comparative Analysis and Beta Feedback
32		Develop Installation Package
33		Integrate Tool with RIMR
34		Demonstrate Final Product
35		Deliver Automated Tool Product
36	3.1.7	**Provide Support for the Automated Tool**

Figure 5 – Schedule for Automated OCTAVE Tool Effort

Issues / Dependencies

- Resource Requirements: The Automated Tool will not require the MTF to purchase any additional equipment or software for Tool execution.
- MISRTs Participation in Beta Testing: The development schedule for the Automated Tool could be impacted unless MISRTs/sites have been recruited and are ready to initiate execution of their sites' risk analysis using the Tool at the times, and for the project durations, indicated in the Tool development schedule or, conversely, the decision is made not to use live sites for operational beta testing. ATI will work with TATRC to predict the necessary timeframes and support DHIAP trainers and leaders as appropriate in site recruitment activities.
- Acquisition of Supporting Software/Hardware Depends on Project Decisions: There are co-dependencies and shared needs for tools and equipment between the Automated Tool development and the Risk Database (RDB) development. The development teams are closely associated and developers' expertise will be applicable across projects. This co-dependence and sharing may affect acquisition schedules.

DHIAP Phase III Technical Development Plan

- Participation in Design Reviews: There are a number of joint reviews scheduled to support continuous communication between developers and stakeholders. The project should be managed in such a manner that requirements for guidance and/or decisions are facilitated by early communication of background material and provision for alternative work pending approval or guidance. In some cases, an accelerated decision process may be necessary to keep the project on track.

- Effect of Unknowns on Schedule/Scope of an R&D Effort: Since the development of the Automated Tool is a research and development task, it is possible that important issues could arise during the design, development, prototyping, testing, and (less likely) refinement steps of the work plan. The DHIAP Team will identify potential risks as early in the process as possible and will work with appropriate resources (Team leaders, TATRC, etc.) to resolve or manage potential risks.

- Integration with Other Efforts:

- The integration of the data collected from the Automated Tool into the RDB depends upon close cooperation of the teams developing the Tool, the RDB, and RIMR. The Tool and RDB development teams have built communication checkpoints into their work plans; they will work with TATRC and other designated resources as appropriate to assure coordination with RIMR support staff as well.

- The integration of DITSCAP, Best Practice, HIPAA, JCAHO and other requirements into the Automated Tool's data collection capability depends upon availability of the results of these investigations and Technical Management/TATRC direction on specific features to be incorporated into the Tool. If TATRC and the DHIAP Team should identify any new features for inclusion in the Tool, the Tool developers will evaluate and prepare high-level design requirements for the changes, identify whether incorporating the requirements into the Tool would have any effect on budgets and schedules, present the assessment to TATRC and DHIAP Technical Management for review, and then comply with the Technical Management/TATRC decision on whether to modify the Tool immediately or defer the change to a later time.

Deliverable

- PC-based Automated OCTAVE Tool (i.e., graphic user interface tool that supports OCTAVE Methodology and includes data transfer capability)

Travel

Most of the travel for this effort involves coordination among the Tool and RDB development Teams, the SEI, and coordination with TATRC. It is anticipated that the planned coordination meetings can occur in conjunction with other planned and programmed travel, hence a consolidated projection of travel is provided following the RDB section.

Equipment

Due to the tight integration of the Tool development and the RDB development, a consolidated projection of hardware and software is provided following the RDB section.

Participant Roles

This task will be led by ATI, and augmented as required by KRM Associates and SEI.

- **ATI** will provide project management and will serve as the technical developer of the Automated Tool.
- **KRM** will provide support throughout the project, particularly in the aspects of functional requirement development and design specification that ensure the Automated Tool's compatibility with the Risk Database.
- **SEI** will provide verification and validation of the functional requirements and technical specifications, subject matter expertise for the Tool's design, and assistance in testing to ensure the preservation of the OCTAVE process.

3.2 Risk Database

(Requirement 1.1)

This portion of the OCTAVE TOOLS effort develops the Risk Database (RDB), a repository for OCTAVE data that is provided via interface with the Automated OCTAVE Tool by MTFs following completion of information assurance risk assessment activities at their sites. The RDB will be designed to support the data analysis and consolidation required for DOD to investigate systemic information assurance risks. The initial RDB will be organized around the OCTAVE-defined data components such as asset, threat, vulnerability, security requirement, etc. Implementation of additional data components and relationships will be assessed for the potential to accommodate HIPAA, JCAHO, and DITSCAP requirements in the RDB.

Methods for accessing the RDB will be designed and developed through this task. The RDB may be accessed via the RIMR web server, or alternative approaches will be developed dependent on the security, policy, and technical requirements. RDB structure will be closely aligned with the information-generation capability of the Automated Tool (Task 3.1, above). The RDB will define the primary data to be transferred from the Automated Tool. Because of the requirements for coordinated processing, the efforts of the RDB Team and Automated Tools Team will be highly coordinated.

Lead Organization

ATI

Participants

KRM Associates, SEI

Background

Successful development and implementation of a Risk Database will provide the capability for a system-wide vision of the risks facing the MTFs. Analysis of the consolidated data by program and project managers able to affect change can dramatically increase the safety and security of sensitive data in the military healthcare system.

Major Activities

3.2.1 Specify System and RDB Capability Requirements

Requirements for the RDB were derived from user requirements (based on input from TATRC, working with and representing the user community, obtained primarily during October and November 2001 meetings with TATRC) and consist of functional, technical, and operational capabilities/requirements. Because the output of the Automated Tool will be the source of input to the RDB, definition of both functional and technical requirements for the RDB were closely coordinated with the Automated Tool effort.

Development of functional capabilities included analysis efforts necessary to determine how multiple instantiations of OCTAVE site data are to be captured, addressing the interface and interaction with the RDB for both the operational users and the support staff (i.e., database administrators), and determining what reports the RDB will be capable of generating. Functional capabilities also include analysis and specification of the user interface to the RDB for extracting information from the RDB.

Development of technical requirements is based on the functional capabilities. Analysis of the functional capabilities of the RDB, requirements of the RIMR operating environment, and capabilities of the COTS tools available for use allowed technical and operational requirements definitions that outline characteristics required for RDB data storage and retrieval, interfaces with other systems and data bases (e.g., with the Automated Tool), security, and report capability.

This section describes the requirements to design and develop the RDB. The requirements identified in this document are based upon the following fundamental requirement:

> *The RDB will allow users (as authorized by the DOD) to analyze data collected from sites' execution of OCTAVEs.*

The system requirements are described in terms of functional capabilities, technical requirements, and operational requirements. User requirements primarily influence the functional capabilities, which describe what the RDB must "do." Functional capabilities will also identify particular functional quality assurance attributes, which the RDB should possess. Technical requirements focus more what the RDB needs to operate, in terms of the computer/server on which the RDB is installed, the operating system, and the application. Operational requirements consist of the performance and physical characteristics and operational conditions within which the product must perform.

This section first establishes the foundation upon which the system requirements will be developed by listing a set of design assumptions. Following those assumptions are the functional capabilities, technical requirements, and operational requirements. The section concludes with an outline of the user documentation, which includes installation and operation guidance, etc., that will accompany the RDB.

3.2.1.1 Assumptions

- The data stored in the RDB is a collection of individual site submissions
    - The Automated Tool user will, by default setting in the Automated Tool, upload all locally collected data to the RDB
    - As an option, the Automated Tool user may select the data that is sent
        - Minimum upload will be the demographic data and acknowledgement of completion of the OCTAVE
        - Selectable options will be the other logically grouped groups of data (e.g., APW(s), vulnerabilities and components scanned, workshop attendees, etc.)
    - As a starting point, the RDB must be capable of managing independent OCTAVE data for approximately 500 site submissions (approximately 160 facilities), and up to 50 concurrent users
- The RDB will be developed in Oracle 8i; RIMR supports Oracle 8i, but not ancillary tools (e.g., Oracle Forms, Reports, and Graphics); RIMR also uses ColdFusion Server

4.5 and ColdFusion Studio 4.5.2, with plans to upgrade to ColdFusion Server 5.0 sometime in 2002

- Security of the RDB, once deployed to RIMR, will be provided by RIMR, to include:
  - Security of the data stored
  - Security of data access
    - RDB user authorization and authentication
    - Role definitions and access controls
  - Security of data transfer from the Automated Tool to the RDB (128 bit SSL); RIMR uses VeriSign
- TATRC, working with the Tiger Team, will define the RDB "user," but in order to set initial user expectations for the RDB, the following basic assumptions apply:
  - Types of RDB users
    - **Database Administrator** – this is a RIMR system/database administrator, operator, and/or developer with full access to the RDB structure and data; these personnel will likely assume the long-term maintenance and support for the RDB
    - **Operational User** – this group will use the RDB for analysis of the data contained within the RDB
  - RIMR will provide access controls for the types of users
  - Operational users have an understanding of the data collected with the RDB

3.2.1.2 Functional Capabilities

- Physical characteristics
  - The RDB database will be designed and developed in Oracle
  - The user interface will be browser based (e.g., ColdFusion and/or HTML)
  - The Automated Tool will provide (via secure upload of site collected OCTAVE data) the data to populate the RDB
    - The Automated Tool will collect the OCTAVE data and send the data to a holding area (where it can be validated)[30]
    - Once validated (by, for example, a RIMR database administrator or DOD designee), the data will be added to the RDB
  - The RDB will be capable of establishing and maintaining multiple versions of data based on different versions of the data captured by the Automated Tool
- Operational User capabilities
  - Operational users will be capable of retrieving RDB data for analysis, but not adding to, editing, or corrupting RDB data
  - The system will provide a consistent, browser-like user interface
  - Data retrieval functions and output – the user will be capable of analyzing and retrieving data in:

[30] Note: As far as the Automated Tool user is concerned, the data is sent to the RDB.

- Commissioned and standard formats[31]
  - The user interface will provide an index of these reports
- Ad hoc reports based on the user-formed queries, such as:
  - MTF OCTAVE participation
  - Data summaries and trends
    - Assets, risks, mitigation plans
    - Protection strategies
    - Vulnerabilities
    - Survey results
  - Site-level draft OCTAVE Final Reports
  - Submissions grouped by time
- Users will need to be familiar with the RDB schema in order to effectively conduct advanced database queries; however, standard reports will be available for users with minimal
- An online "Suggestion Box" will provide a mechanism for users to provide comments and user evaluations to the system administrators

- Database Administrator capabilities
  - Direct data entry and validation of data for the RDB will be available for database administrators via the console and/or controlled access interface
  - Minimal training requirement: one-two days of orientation (concurrent with installation at RIMR) should be sufficient to learn to support the system
- Data definition and database requirements
  - The data dictionary/schema for the RDB will be based on that of the Automated Tool and support multiple instantiations of OCTAVE site data
- Data verification/validation functions – the RDB will provide a data holding area for the database administrator to review (and edit, based on procedures developed) the data submitted by a site prior to accepting it and passing it to the RDB
  - Once the database administrator validates and verifies the uploaded data (from a site's submission via the Automated Tool), the data will be added to the RDB
    - The database administrator will have the capability to edit (add, correct, delete) database records via standard SQL commands
    - The date of update/entry will be captured
    - The data will be entered, stored, and retrieved in an organized fashion; the RDB system will assure that the data is delivered to the right data field in the database; data fields will be predefined where appropriate and categorized in an analytically and administratively useful structure

[31] The content of some standard reports will be fairly straightforward and the DHIAP Team will draft those for TATRC's review. For other reports, TATRC, working with the Tiger Team, will provide report descriptions.

- Data standardization will be achieved by capturing the version of the Automated Tool used to collect the site OCTAVE data
- *Assumptions*
  - The database administrator will verify that the uploaded data from the Automated Tool is complete and correct
    - The Automated Tool, for its part, will allow the user to edit and correct data prior to upload
  - The database administrator will verify that all the available data has been captured and added to the RDB
  - The database administrator will verify that the data output requirements have been included during the entry process

3.2.1.3 Technical Capabilities

- Computer resource requirements
  - The RDB server will, at a minimum, be comparable to the following system: Pentium III, 933 MHz, 256 kB Cache, 48x20x CD ROM, 256 MB RAM, 30GB Hard Drive
    - 10/100 Ethernet Server Adapter
    - 15 inch Monitor
  - The server's operating system will be Windows 2000 Server, for at least five concurrent accesses, and with the Resource Kit
  - The RDB application will be an Oracle database
  - The user interface to the RDB will be browser-based using ColdFusion and standard HTML
- External interfaces
  - Console interface for database administrators
  - Secure web access for RDB users
  - Secure upload of site collected OCTAVE data from a site's Automated Tool; encrypted, using at least 128 bit SSL
- Installation and maintenance
  - The RDB will be delivered to TATRC and the RIMR team who will integrate it into the existing RIMR structure and provide continued support
  - Low software maintenance will be a design objective; any maintenance tail will be defined (e.g., if there is an annual maintenance fee with Oracle 8i)
  - Version/configuration control reside with RIMR

3.2.1.4 Operational Capabilities

Operational requirements consist of those organizational, operational user, maintenance, and security requirements necessary to support fulfillment of the system's objectives.

- Organization requirements (see Assumptions above)
  - RIMR provides the environment to support the RDB
    - Oracle, ColdFusion, and web servers

        - Security of the RDB server and the data stored in the RDB
        - Security of the data transfer from the site to the RDB (SSL)
        - User authentication, authorization, and access control to the RDB
        - Long-term maintenance of the server and the RDB
- Operational user requirements (see Assumptions above)
    - Basic understanding of the data OCTAVE collects
    - User account privileges to access RDB
- Security and privacy
    - Data security will be a design consideration; to the extent that the RIMR site, the operating system (with appropriate patches), Oracle, and ColdFusion are capable of providing security, the RDB will support (and not degrade) the security requirements of RIMR
    - The RDB and its data will be physically secure to the extent that the server upon which it is loaded are secured by the site
    - Secure upload of site OCTAVE data from the Automated Tool will be accomplished with 128 bit SSL
    - Based on controls provided by RIMR, the RDB user will access only authorized OCTAVE records

3.2.1.5 User Documentation

- Operational User documentation (to use the RDB)
    - Getting Started
        - Finding information (e.g., explanation of font and format in user documentation)
        - Using the RDB
    - Database Command Reference
    - How to Obtain Help
- Administrative User documentation (to maintain and support the RDB)
    - RDB installation and maintenance procedures
- Technical documentation and user documentation will be delivered with the RDB

The RDB Team conducted formal reviews (October and November 2001) of the requirements developed above with TATRC and the rest of the DHIAP Team and obtained and incorporated feedback on the recommendations, assumptions, and design decisions. During the November meeting, the Team also confirmed appropriate portions of RDB requirements with RIMR support staff. The Team will continue to accept guidance from TATRC and the Military Health System's RDB Advisory Group to assure consistency of DHIAP plans with the needs of these organizations.

3.2.2 Select Development Environment

In order for the RDB to be integrated with existing DOD systems and to minimize the training and maintenance burdens placed on DOD support personnel, Oracle8*i* and its associated tools will be used as the database development and support software. The RDB will be developed so that it will be maintainable by a database administrator experienced in Oracle. In order to meet the technical requirements, tools such as Cold Fusion, Visual Studio, etc. may be necessary to support the implementation of the RDB.

3.2.3 Develop Architectural Design

Communication among the designers of the RDB, the Automated Tool, and other key stakeholders is facilitated with a clear picture of the intended architecture of the system and the RDB's relationship to that system. The architecture of a database is a means of depicting design decisions. Using the functional and technical requirements and the technical criteria of the selected COTS development tools, the Team will develop a top-level architectural design for the database and the supporting capabilities (data interface, user interface, component interfaces). Upon completion of the design, ATI will conduct a design review with TATRC and update the design, as appropriate, based on results of the meeting.

3.2.4 Develop Test Plan

The Team will develop a plan for validating the functionality of the RDB against the functional and technical requirements. The plan will include qualification testing, i.e., testing capabilities against requirements. This will include testing functions planned for both the user community and the support staff, and will call for these functions to be tested both "locally" and "from a distance," as appropriate, to how the RDB will be used in a live environment. The test plan will include components to be executed in concert with other technical projects, such as testing of data upload to the RDB from the Automated Tool and testing of all RDB. As the components of the RDB are developed, the test plan will be updated.

3.2.5 Design and Create the Database Structure

The Team will apply their knowledge of the RDB requirements, RDB environment, Automated Tool environment, and the OCTAVE process to design the logical and physical structure to be used by the Oracle implementation of the RDB. We anticipate that the requirements and the architecture will specify a database structure designed to allow, as much as possible, for additional mappings between the data and DITSCAP, Best Practice, HIPAA, and JCAHO requirements which may be available at a later time. Design consideration will also be given to DOD's potential need to isolate data by categories (e.g., by service). The Team will document the detailed database design by generating a schema and data dictionary as part of the database structure creation, and will make these documents available to the Automated Tool Team and TATRC upon their creation and as changes are made during later RDB development activities.

3.2.6 Design and Develop the RDB User Front-end (Web Interface)

The Team will design the RDB's front-end application based on use the functional and technical requirements. The application (called the "Web Interface" in Phase III requirements and proposal documents) will support user access to the RDB both remotely via the web and locally via intranet or direct access. We anticipate that the requirements and the architecture will specify components for access by reporting entities (i.e., uploading the OCTAVE data from the MISRTs), end users (e.g., to support query and/or reporting of information contained in the RDB), and for access by technical staff who support the RDB (e.g., to support maintenance of user access profiles, maintenance of the data dictionary, etc.). The design effort will include analysis of security, policy, and technical requirements to determine specific design approaches and will consider both on-line via web access and intranet or direct access to provide a web-like look and feel. Following a review of the design with TATRC and other appropriate stakeholders, the Team will develop a prototype of the front-end application.

3.2.7 Develop Report Functions

The Team will develop the RDB report capabilities as outlined in the requirements specifications. Also in this effort, the Team will assure that the reporting functions are capable of providing user-developed reporting as specified in the functional requirements. They will also assure that functions to support placing security and policy constraints on users' report creation capabilities (e.g., based on database queries) operate as planned. They will create an index of reports (i.e., a group of queries that each produce a specified "standard report"), create a method for users to access the index, and prepare documentation of both the standard reports and the method for having them executed.

3.2.8 Test, Demonstrate, and Enhance the Risk Database

The Team will test the RDB and its user access components during their development. They will test the functionality of all components working together in a laboratory environment. Following this testing, they will conduct two types of demonstrations for the other members of the DHIAP Team and TATRC. The first is a prototype demonstration to show the capabilities of the RDB and its interfaces and to identify any issues or inappropriate limitations of the RDB. Issues identified during the demonstration will be documented for consideration in enhancing the system.

The Team will evaluate the feedback obtained about the RDB's usability and technical features, and classify the recommendations for immediate action vs. deferral as "nice-to-have" in a post-Phase III version. They will present the results of their evaluation to TATRC and work with TATRC to determine what changes, if any, should be made to the toolset. They will then modify RDB functionality and validate the RDB in the laboratory environment.

Following successful lab testing, the Team will demonstrate the RDB functionality to TATRC, this time with other appropriate DOD stakeholders invited by TATRC to participate. This testing will be in preparation for migration of RDB functionality to RIMR and the DOD. This test will include execution of the data submission procedures.

3.2.9 Develop RDB Management Guidelines Document

Concurrent with testing the RDB and its interfaces, the Team will prepare various types of system documentation that they will bind together in an "RDB Management Guidelines" document. The Guidelines components developed in this effort will include:

- Instructions for Submitting, Approving, and Entering Data to the Database;
- Security Policy, Procedures, and Practices that are Appropriate for RDB Support;
- Job Responsibilities and Authorities for the RDB Manager; and
- Requirements to Maintain, Sustain, and Update the RDB.

  The Team will develop operational requirements to maintain, sustain and update the RDB. This will include information on the schema, making changes to the database structure, ensuring valid data entry, and backing-up the information in the database. The Team will develop and provide operational instructions on operations and maintenance of the RDB. The instructions will include database server instructions as well as necessary instructions to facilitate administration of the RDB. Data base administration requirements are projected to include database security, backup and recovery, report maintenance, data quality criteria, and data purging. Applicable procedures will be developed and documented during the laboratory testing and initial fielding of the RDB.

- Standard Operating Policies and Procedures

  In collaboration with the RIMR administrators, the DHIAP Team will develop operating procedures and general support procedures for the RIMR RDB. The Team will work with RIMR technical staff to assess technical and procedural risks at the site and with data transfer (upload and download) of potentially sensitive data. The Team will collaborate with RIMR staff to develop recommended practices and procedures for assuring database security and for controlling access as appropriate for the resource's diverse support and user community. The procedures refined in transferring the RDB to the RIMR will be incorporated into the recommendations for the RDB Standard Operating Procedures and RDB Security Policy.

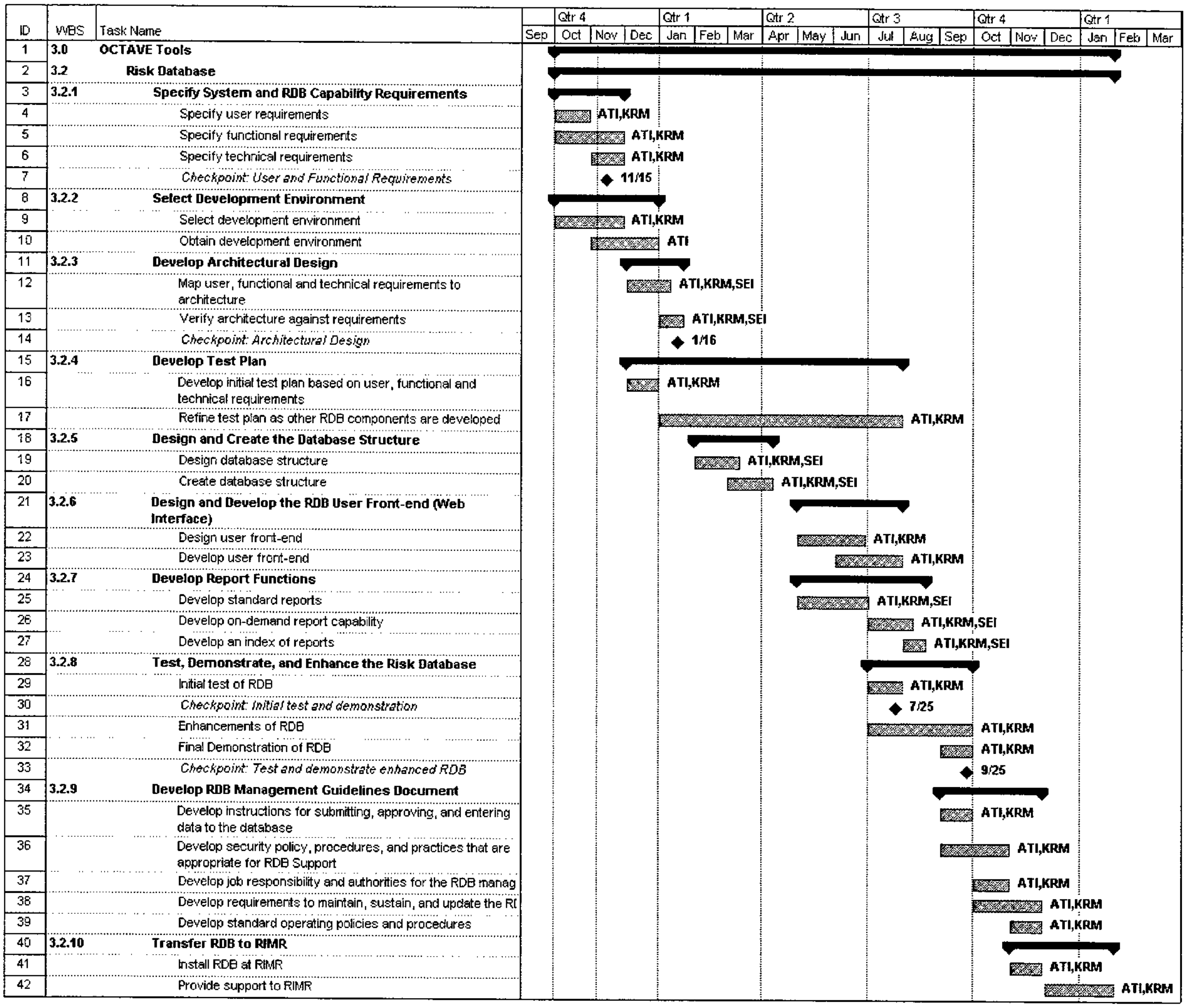
3.2.10 Transfer RDB to RIMR

Following the initial RDB demonstration to TATRC, the Team will begin working with RIMR operational staff to develop a migration plan for transition of the RDB to RIMR. Following completion of the second RDB demonstration to TATRC and RIMR staff, they will execute that migration plan to accomplish RDB transfer to RIMR and, working with RIMR and TATRC staff, test the resulting RDB implementation on RIMR. When testing has been successfully completed, the Risk Database and all associated documentation will be transferred to RIMR for full implementation. Support advice and assistance will be provided for use and maintenance of the RDB until contract completion.

DHIAP Phase III Technical Development Plan

Schedule

Figure 6 below indicates the activities, planned timeframes, and participants of the major activities of the Risk Database effort.



ID	WBS	Task Name
1	**3.0**	**OCTAVE Tools**
2	**3.2**	**Risk Database**
3	**3.2.1**	**Specify System and RDB Capability Requirements**
4		Specify user requirements
5		Specify functional requirements
6		Specify technical requirements
7		*Checkpoint: User and Functional Requirements*
8	**3.2.2**	**Select Development Environment**
9		Select development environment
10		Obtain development environment
11	**3.2.3**	**Develop Architectural Design**
12		Map user, functional and technical requirements to architecture
13		Verify architecture against requirements
14		*Checkpoint: Architectural Design*
15	**3.2.4**	**Develop Test Plan**
16		Develop initial test plan based on user, functional and technical requirements
17		Refine test plan as other RDB components are developed
18	**3.2.5**	**Design and Create the Database Structure**
19		Design database structure
20		Create database structure
21	**3.2.6**	**Design and Develop the RDB User Front-end (Web Interface)**
22		Design user front-end
23		Develop user front-end
24	**3.2.7**	**Develop Report Functions**
25		Develop standard reports
26		Develop on-demand report capability
27		Develop an index of reports
28	**3.2.8**	**Test, Demonstrate, and Enhance the Risk Database**
29		Initial test of RDB
30		*Checkpoint: Initial test and demonstration*
31		Enhancements of RDB
32		Final Demonstration of RDB
33		*Checkpoint: Test and demonstrate enhanced RDB*
34	**3.2.9**	**Develop RDB Management Guidelines Document**
35		Develop instructions for submitting, approving, and entering data to the database
36		Develop security policy, procedures, and practices that are appropriate for RDB Support
37		Develop job responsibility and authorities for the RDB manag
38		Develop requirements to maintain, sustain, and update the RI
39		Develop standard operating policies and procedures
40	**3.2.10**	**Transfer RDB to RIMR**
41		Install RDB at RIMR
42		Provide support to RIMR

Figure 6 – Schedule for Risk Database Effort

Issues / Dependencies

- <u>Integration with Other Efforts</u>:

- The integration of the data collected from the Automated Tool into the RDB depends upon close cooperation of the teams developing the Tool, the RDB, and RIMR. The Tool and RDB development teams have built communication checkpoints into their work plans; they will work with TATRC and other designated resources as appropriate to assure coordination with RIMR support staff as well.

- The integration of DITSCAP, JCAHO, HIPAA, and other requirements into the RDB capabilities depends upon (1) availability of the results of these investigations and (2) Technical Management/TATRC direction on specific features to be incorporated. When any new features have been identified, the RDB developers will evaluate and prepare high-level design requirements for the changes, identify whether incorporating the requirements into the

DHIAP Phase III Technical Development Plan

RDB would have any effect on budgets and schedules, and then act accordingly after Technical Management/TATRC decide whether to modify the tool immediately or defer the change to a later time.

- Timeline: The timeline described is aggressive and has dependencies on the OCTAVE Automated Tool, the joint reviews, and the checkpoint decisions. Successfully meeting project timelines will depend rapid turnaround on design approval, availability of TATRC, RIMR, etc. for coordination and concurrence, and the availability of others as required and/or desired.

Deliverables

- RDB Functional and Technical Designs and List of Assumptions
- RDB Information Model and Architecture
- RDB Standard Operating Procedures
- RDB Security Policy
- Risk Database (server hardware and software)
- RDB report retrieval capability, including standard and commissioned reports

Consolidated Travel for Risk Database and Automated Tool Efforts

Most of the travel for this effort involves coordination among the Automated Tool and RDB development Teams, the SEI, and coordination with TATRC. To reduce expenditures for travel, the Team will try to assure that these coordination meetings are timed to coincide with other planned travel (e.g., for Interim Program Reviews and other joint Team events). Table 3 below, therefore, provides a travel projection that is consolidated for the Risk Database and Automated Tool efforts.

Table 3 - Proposed Travel for Risk Database and Automated OCTAVE Tool Efforts

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Oct-01 O1	Charleston, SC w/ M4	AT and RDB: Develop User Requirements, Functional and Technical Capabilities/Requirements Specifications	KRM	1
Nov-01 O2	Washington, DC w/ M5, T4, B1	AT and RDB: Checkpoint with TATRC on User Requirements and Functional Capabilities	ATI, KRM	4
Dec-01 O3	Charleston, SC	AT: Specify Requirements RDB: Select Development Environment and Develop Architectural Design	KRM	1
Jan-02 O4	Charleston, SC M6, T5, B2	AT and RDB: Checkpoint with TATRC on Requirements	ATI, KRM (TATRC)	1
Feb-02 O5	Charleston, SC	AT: Develop System and Software Architectural Design RDB: Develop Test Plan and Design and Create Database Structure	KRM	1

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Mar-02 O6	Charleston, SC B3	AT: Checkpoint with TATRC on Design RDB: Design and Develop RDB User Front-end	KRM	1
Jun-02 O7	Charleston, SC w/ M7	AT: Perform Software Coding, Testing, and Integration RDB: Design/Develop RDB User Front-end and Develop Report Functions	ATI	1
Jul-02 O8	Charleston, SC w/ B6	AT: Demonstrate Prototype Automated Tool to TATRC RDB: Checkpoint with TATRC on Initial Test and Demonstration of the RDB	KRM, (TATRC)	1
Aug-02 O9	Charleston, SC	RDB: Test, Demonstrate, and Enhance the RDB and Develop Report Functions	KRM	1
Sep-02 O10	Charleston, SC w/ M8	AT: Checkpoint with TATRC on Functionality (prior to Beta testing) RDB: Checkpoint with TATRC to Test and Demonstrate Enhanced RDB AT: Refine Tool and Develop Installation Package RDB: Develop RDB Management Guidelines Document	KRM, (TATRC)	1
Nov-02 O12	Washington, DC	AT: Checkpoint with TATRC on Functionality (after Beta testing) RDB: Transfer to RIMR	ATI, KRM	3
Jan-03 O13	Washington, DC w/ M9	AT: Demonstrate Final Product Automated Tool to TATRC as a fully packaged application, and turn over to RIMR	ATI, KRM	3

Consolidated Equipment for Automated Tool and Risk Database Efforts

This equipment section identifies the types of software and hardware that may be necessary to build the Automated Tool and the Risk Database. The approach is for a development platform to be purchased and used throughout the design, development, and testing periods. Later, another (more current) system will be purchased, and when all products have been deemed functionally capable, they will be moved to this production system. The goal is to deliver the product(s) on the most capable and up-to-date system available (within budget).

The equipment requirements to support the Automated Tool development will consist primarily of the software tool(s) used to develop the product. The effort will leverage other support requirements (e.g., server) via coordination with the RDB development effort. The actual product(s) to be purchased for this effort will not be determined until the Functional Requirements, Technical Specifications, and Product Selection activities have been completed; however, an example of the software and the estimated costs are presented in Table 4 below.

DHIAP Phase III Technical Development Plan

Table 4 - Example of Materials for Risk Database and Automated OCTAVE Tool

Risk Database Server Hardware	
IBM xSeries 200 PIII, 933 MHz, 256 kb Cache, 48x20x CD ROM, 64 MB • 30GB, 7200 rpm ATA/100 (EIDE) Hard Drive • 10/100 Ethernet Server Adapter • IBM 10/20GB NS Internal SCSI Tape Drive (SL) • PCI Ultra 160 SCSI adapter • 512 MB 133 MHz SDRAM unbuffered DIMM upgrade • APC Smart UPS 1400 • 17 inch G74 Monitor • Windows 2000 Server for five concurrent accesses	Note: two (2) each – one for development and support, one for deployment to RIMR
Oracle Database Software for RDB	
Oracle Database 8i Release 3 (8.1.7) CD Pack for MS Windows • Oracle Database Standard Edition, Named User Two Year • Update Subscription Service - Oracle Database Standard Edition Named User Two Year for 2 years • Product Support - Oracle Database Standard Edition Named User Two Year for 2 years • 8.1.7 Oracle8i On-Line Generic Documentation CD-ROM Release 8.1.7 • 8.1.7 Oracle8i Supplied Java Packages Reference Release 8.1.6 • 8.1.7 Oracle8i SQL Reference Release 8.1.7 (2 volumes) • 8.1.7 Oracle8i Supplied PL/SQL Packages Reference Release 8.1.6 (2 volumes) • 8.1.7 Oracle8i Administrator's Guide Release 8.1.6 • 8.1.7 Oracle8i Utilities Release 8.1.6 • 8.1.7 Oracle8i Backup and Recovery Release 8.1.6 • 8.1.7 Oracle8i Error Messages Release 8.1.6 (3 volumes) • 8.1.7 Oracle8i XML Reference Release 8.1.7 (2 volumes) • 8.1.7 Oracle8i Supplied Java Packages Reference Release 8.1.7 • 8.1.7 Oracle8i Application Developer's Guide - XML Release 8.1.7 (2 volumes) • Oracle Internet Developer Suite	RDB database and support
Automated Tool	
• MS Office 2000	Access, Excel, FrontPage, Word, Outlook, PowerPoint
• MS Visual Studio Professional 6.0 w/ Plus Pack	Five Visual development tools (VB, J++, C++, FoxPro, InterDev) with enhanced support for SQL Server and Oracle
• DemoShield	Fourth Generation Development tool
• InstallShield Developer	Create installation package

Miscellaneous and Shared Components

• Linksys 5-port 10/100Base-TX Fast Ethernet Managed Hub	
• CAT5e RJ45M 10' cable	
• HP Laserjet 1200 Printer	
• Windows 2000 Server Additional 5 client access license (5*30)	
• Windows 2000 Server Resource Kit	
• Windows 2000 Server Resource Kit Supplement One	
• Norton AntiVirus 2001 7.0	Virus Protection
• MS Visual Studio Professional 6.0 w/ Plus Pack	Five Visual development tools (VB, J++, C++, FoxPro, InterDev) with enhanced support for SQL Server and Oracle
• Visio 2000 Professional Edition	Graphics Package - Entity Relationship Diagrams, Data flow diagrams, network diagrams
• ColdFusion Server 5 and support	Webserver supporting ColdFusion extensions and database interfacing.
• ColdFusion Studio v4.5, Ultra 4 Studio	Environment for the development of applications on the ColdFusion server
• Verisign Digital Certificate for servers	Secure Upload for OCTAVE data

Participant Roles

This task will be led by ATI, augmented as required by KRM Associates and SEI.

- **ATI** will provide project management and will serve as the technical developer of the Risk Database.
- **KRM** will provide support throughout the project, particularly in the aspects of functional requirement development and design specification that ensure the RDB's compatibility with the Automated Tool.
- **SEI** will provide verification and validation of the functional requirements and technical specifications, subject matter expert advice on the design, and assistance in testing to ensure the preservation of the OCTAVE process.

DHIAP Phase III Technical Development Plan

4 OCTAVE Comparative Analysis

This task consists of two major subtasks: Conduct Comparative Analyses and Develop OCTAVE Tailoring Recommendations.

(Requirement 1.2.1a)

The DHIAP Team will develop recommendations and guidance on how the OCTAVE Method might be tailored and applied more effectively to support or complement the requirements of DITSCAP, HIPAA policy, relevant JCAHO policy, and industry best practices.

(Requirement 1.2.1b)

The DHIAP Team will use the material gathered in the activities associated with training and fielding OCTAVE to DOD MISRTs to develop recommendations for tailoring approaches to meet DOD specific objectives.

Lead Organization

ATI

Participants

SEI, (TATRC)

Background

As part of the Department of Defense and the medical community, military healthcare facilities are subject to the laws, policies, and regulations of both organizations. As such they are subject to periodic inspections to ensure their compliance to applicable policies and laws mentioned above. Currently there is no "silver bullet" that identifies overlaps in these policies. As an excellent tool for threat, asset, and vulnerability identification, security policy development, and risk planning, the OCTAVE Method does overlap and complement many of those policies and laws pertinent to the defense healthcare community. However, there currently is no formal OCTAVE documentation that explicitly details these overlaps in policy compliance and industry best practice.

The OCTAVE Method is designed to assess many different asset and threat scenarios. As it was designed to address a wide range of industries employing the use of information technology assets, including both commercial and government organizations, no guidelines are currently available on tailoring OCTAVE to address issues common and specific to DOD issues.

Major Activities

4.1 Conduct Comparative Analyses

The DHIAP Team will work with TATRC to identify and analyze gaps and redundancy between OCTAVE and the following documents:

- DOD Information Technology Security Certification and Accreditation Process, (DITSCAP, DOD Instruction 5200.40), the DITSCAP Application Manual (DOD Manual 8510.1-M), and DISA recommended SSAA output

- Relevant Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Preparation
- Health Insurance Portability Accountability Act (HIPAA) documentation of compliance (when available)
- RFC 2196, The Site Security Handbook. This document serves as a baseline best practice for security policy.

As described in Tasks 4.1.1 – 4.1.4 below, each of these policy, guide, or directive documentation sources will be subject to an individual review and analysis for overlap with the OCTAVE methodology. As each review is completed, areas of that policy or guide documentation that either satisfy an OCTAVE requirement or may be satisfied through conducting an OCTAVE will be documented in a draft comparative analysis document for use by the DHIAP Team and TATRC in determining what types of changes, if any, are appropriate for use in updating the OCTAVE Method for DOD use.

4.1.1 Gather Documentation

The DHIAP Team will gather source documentation for DITSCAP, RFC2196, HIPAA, and JCAHO requirements.

4.1.2 Conduct DITSCAP Review

4.1.2.1 Conduct SSAA Review

Of the above documents and guides, only the DITSCAP process requires mandatory output in the form of the SSAA. The SSAA will allow the DHIAP Team to note specific areas of overlap between the SSAA data, and the data that makes up the OCTAVE Asset Profile Workbook (OCTAVE output). The DHIAP Team will begin its OCTAVE comparison with the DITSCAP SSAA. The analysis of the DITSCAP SSAA will document general overlaps in each section of the SSAA outline to the individual OCTAVE processes or phases. After areas of general overlap are identified and addressed, the DHIAP Team will further analyze the SSAA and the relevant sections of the OCTAVE Method documentation, as well as conduct a gap analysis between areas of input in the SSAA and the OCTAVE Asset Profile Workbook. They will document results and potential recommendations in a draft form for internal review and use in Task 4.1.2.2.

4.1.2.2 Conduct DITSCAP Application Manual Review

Following completion of the SSAA review, the DHIAP Team will analyze the DITSCAP Application Manual as documented in DOD Manual 8510.1-M for areas of guidance and instruction overlap with guidance and instruction present in the OCTAVE documentation. After the initial analysis and development of a comparative matrix are completed, the DHIAP Team will conduct a gap analysis between the DITSCAP guidance and specific OCTAVE guidance. They will document results and potential recommendations in a draft form for internal review and use in Task 4.1.2.3.

4.1.2.3 Conduct DITSCAP Process Review

The DHIAP Team will then analyze the DITSCAP process as documented in DOD Instruction 5200.40 for areas of process overlap with the OCTAVE Method. During this analysis, specific sections of each document will be mapped to appropriate OCTAVE phases and processes in a matrix. After the initial analysis and matrix are completed, the DHIAP Team will conduct a gap analysis between the DITSCAP methodology and specific OCTAVE processes. They will document results and potential recommendations in a draft form for an internal review and use in Task 4.1.2.4.

4.1.2.4 Draft DITSCAP Comparison Summary

The DHIAP Team will use the documentation developed in Tasks 4.1.2.1-4.1.2.3 to draft a white paper that summarizes the comparative analysis of the OCTAVE Method and the DITSCAP process. Following an internal Team review, the white paper will be provided to TATRC for review.

4.1.3 Conduct Best Practice (RFC 2196) Review

The DHIAP Team will apply a gap analysis methodology similar to the process followed with DITSCAP to determine OCTAVE overlaps with industry best practices described in RFC 2196. They will document results and potential recommendations in a draft form for internal review and then use the documentation to draft a white paper that summarizes the comparative analysis of the OCTAVE Method and Best Practice as outlined in RFC 2196. Following an internal Team review, the white paper will be provided to TATRC for review.

4.1.4 Conduct HIPAA Review

The DHIAP Team will apply the same gap analysis methodology to determine OCTAVE overlaps with HIPAA Security requirements (using the final version of the rule if it is available or the Notice of Proposed Rulemaking version if the rule is not yet final). They will document results and potential recommendations in a draft form for internal review and then use the documentation to draft a white paper that summarizes the comparative analysis of the OCTAVE Method and HIPAA Security requirements. Following an internal Team review, the white paper will be provided to TATRC for review.

4.1.5 Conduct JCAHO Review

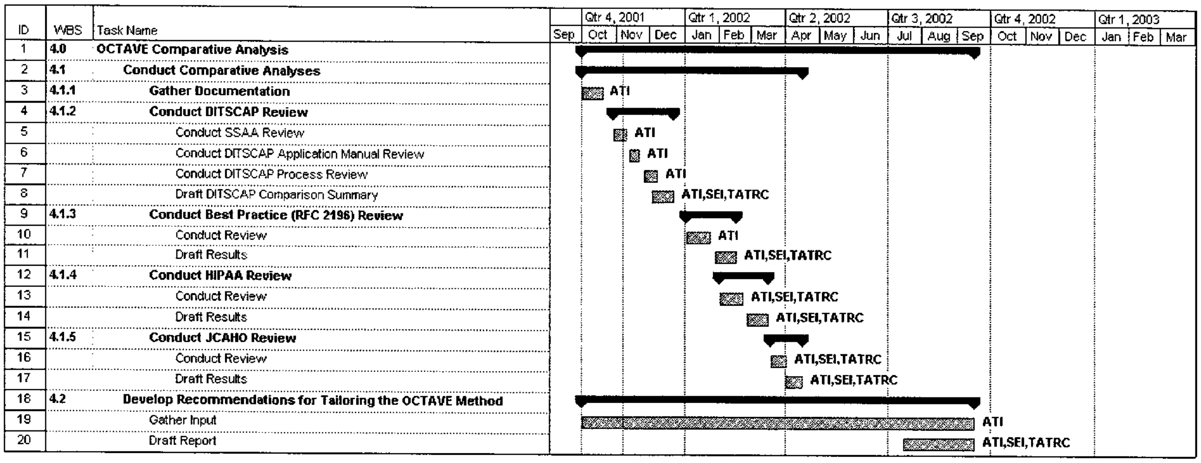
The DHIAP Team will apply the same gap analysis methodology to determine OCTAVE overlaps with JCAHO Information Management requirements. They will document results and potential recommendations in a draft form for internal review and then use the documentation to draft a white paper that summarizes the comparative analysis of the OCTAVE Method and JCAHO requirements. Following an internal Team review, the white paper will be provided to TATRC for review.

4.2 Develop Recommendations for Tailoring the OCTAVE Method

The DHIAP Team will collect recommendations from OCTAVE users to identify outstanding issues. The DHIAP team will identify issues as candidate recommendations for potential enhancements to the OCTAVE methodology, and submit the issues to TATRC.

Schedule

Figure 7 below indicates the activities, planned timeframes, and participants of the major activities of the OCTAVE Comparative Analysis effort.



ID	WBS	Task Name
1	**4.0**	**OCTAVE Comparative Analysis**
2	**4.1**	**Conduct Comparative Analyses**
3	**4.1.1**	**Gather Documentation**
4	**4.1.2**	**Conduct DITSCAP Review**
5		Conduct SSAA Review
6		Conduct DITSCAP Application Manual Review
7		Conduct DITSCAP Process Review
8		Draft DITSCAP Comparison Summary
9	**4.1.3**	**Conduct Best Practice (RFC 2196) Review**
10		Conduct Review
11		Draft Results
12	**4.1.4**	**Conduct HIPAA Review**
13		Conduct Review
14		Draft Results
15	**4.1.5**	**Conduct JCAHO Review**
16		Conduct Review
17		Draft Results
18	**4.2**	**Develop Recommendations for Tailoring the OCTAVE Method**
19		Gather Input
20		Draft Report

Figure 7 – Schedule for the OCTAVE Comparative Analysis Effort

Issues / Dependencies

- Availability of HIPAA Security Standards: If the HIPAA Security Standards have not been finalized, the DHIAP Team will have to use the NPRM version of the standards for their OCTAVE-HIPAA comparison.
- Availability of JCAHO Standards: The DHIAP Team expects JCAHO requirements for information security to align with the emerging HIPAA security rules. Analysis of this aspect will be dependent on availability of clear guidance from JCAHO.
- Availability of Input from OCTAVE Users: OCTAVE users' input into web support tools and survey forms is encouraged, but not mandatory. This could adversely affect the amount of useful feedback reported to the DHIAP Team, as well as have a negative impact on identification of noticeable trends from those sites that have initiated the OCTAVE methodology.

Deliverables

The DHIAP Team deliverables to TATRC will include the following documents:

- Recommendations for Tailoring Baseline OCTAVE to DOD Requirements report (identification of candidate subjects for revision of the OCTAVE Method to include DOD-specific situations based on lessons learned from OCTAVE execution)

Travel

No travel is required to complete the activities of this task.

Equipment

No equipment is required to complete the activities of this task.

Participant Roles

This project will be led by ATI, augmented as required by SEI and TATRC.

- **ATI** will provide project management, conduct the research efforts, lead internal ATI-SEI reviews of the draft results of each analysis effort, and draft the deliverables.
- **SEI** will provide subject matter expertise on OCTAVE and review the comparative analysis white papers as appropriate.
- **TATRC** will provide subject matter expertise on HIPAA and DITSCAP as appropriate.

5 Biometric Authentication Prototype

(Requirement 2.1)

The DHIAP Team will design and demonstrate a biometric prototype system to study the effects of applying biometric authentication modes in an operational MTF environment. This task will build upon and test the findings in the Phase II Business Case Analysis (BCA), *Effective Authentication in a Medical Environment.*[32] Specifically, this task will examine the following two hypotheses:

***H**$_{O1}$*: *When comparing conventional logon/password to a single type of biometric authentication method in a single context, users never prefer biometrics.*

H$_{O2}$: When comparing conventional logon/password to all types of biometric authentication methods in varying contexts, users never prefer biometrics

The results of the demonstration will address whether or not users in operational medical environments will support a biometric over the commonly used password and whether the operational medical environment influences the appropriate choice of the biometric authentication mode (e.g., finger scan, voice, face, or iris). For example, the BCA findings noted that voice recognition is a poor choice in an outpatient clinic because of the background noise – this makes sense and undoubtedly applies to many voice recognition products, but it should be tested and validated with hard data. Likewise, the vendor of iris recognition technology claims to be capable of capturing good data even if a person is wearing glasses, but can that be extrapolated to wearers of protective goggles and/or surgical loupes?

In certain operational environments, does compelling evidence (in terms of user acceptance, security, maintenance, and other factors) exist to replace password authentication with a biometric mode? This is a core issue upon which any eventual migration to biometrics will depend.

Prototyping an authentication system that enables the collection of real-world data to answer these questions will demonstrate the utility and the limitations of the current and emerging biometric technology applied to an operational environment, rather than simply relying upon vendor claims.[33] Capturing the true impact of the operational medical environment will require engagement of a willing and supportive test site, and this will be pursued to the maximum extent possible; however, valid data can still be obtained by simulating the operational environment in a quasi-laboratory setting. This task's side-by-side operational product testing will capture

[32] Pellissier, Stephen V., et al. *Effective Authentication in a Medical Environment.* Business Case Analysis. Advanced Technology Institute. ATI IPT Technical Report 01-01. DAMD17-99-C-9001. January 2001. URL: http://ips.aticorp.org/TR/.

[33] All too often vendor claims of accuracy are not achievable in operational settings. Army Research Laboratory, for example, tested voluntary iris scanning for simulated physical access. The pilot program at ARL reported finding the accuracy of iris recognition (from Iridian) to be much lower than claimed accuracy (roughly 1 error in 20 vs. the claimed 1 error in 1 million).

DHIAP Phase III Technical Development Plan

valuable, unbiased, vendor-neutral data for use by acquisition and policy decision makers. Results may also include a suite of demonstrable artifacts.

Lead Organization

ATI

Participants

BWXT Y-12 LLC and KRM Associates

Notional System Description

The DHIAP Team will continue the investigation started in the BCA; that is, determine which biometric authentication method is most suitable in the various MTF operational environments and whether biometric authentication is better (in terms of user acceptance, accuracy, security, maintenance) than passwords. In order to accomplish this, the Team will not only develop the interfaces necessary to integrate the selected biometric products into an Windows NT/2000 workstation, but also the engine to collect the study data generated from each authentication attempt.

As indicated in Figure 8, the "system" would conceptually consist of a Windows NT/2000 workstation with a variety of biometric devices available, so the user can choose the method of authentication. In the background, the system will capture parametric information (e.g., success/failure of authentication, time required to authenticate, etc.) that the Team can use to make quantifiable comparisons of the methods.

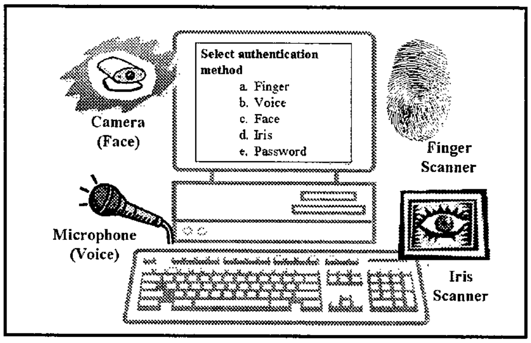


Figure 8 – Biometric Authentication Prototype Test Station

Background

In today's medical environment, virtually all medical information is stored electronically. Unfortunately, this availability also exposes the medical community to a variety of new threats that can have impact on the confidentiality, integrity, and availability of information. Information assurance has become a great concern to the medical community.

As the method of identifying authorized users and allowing them access to network/computing resources, authentication is an integral part of information protection. Traditional authentication has consisted of passwords that are often shared or can be easily cracked using malicious tools easily obtainable on the Internet. MTFs need a better way of authenticating authorized users, and biometric authentication offers a possible solution.

Major Activities

The major activities in this task are outlined below. Iterative refinement of the prototype design and development, along with periodic "checkpoints" to ensure the products meet Government expectations along the way, will be key to achieving operation success, capturing useful data, and meeting customer satisfaction.

5.1 Select Parameters to Evaluate

The DHIAP Team will identify the parameters against which the methods of authentication will be evaluated. The table below illustrates some (i.e., not a complete list) of the evaluated parameters.

Parameter	Evaluation Criteria	Comment
Enrollment	• Success Rate • Time Required • Time Until Re-enrollment	All biometrics require a user to enroll, and since a template ages with time, periodic re-enrollment is necessary.
Authentication	• Accuracy, in terms of: o Success/Failure o False Accept Rate o False Reject Rate • Time to Authenticate	Success/Failure and Time to Authenticate can be used to compare biometric methods to password authentication. FAR and FRR can be used to compare biometric methods.
User Acceptance	• Intrusiveness • Ease of Enrollment • Ease of Authentication	Which method of authentication does the user prefer?
Technical Requirements and Maintenance	• Support in terms of manpower and cost • System requirements • Training • Scalability	Which method of authentication is easiest to support?
Cost	• Cost to purchase • Cost to maintain • Recurring costs	Which is the most cost effective method?
Security	• Security will primarily be assessed in terms of authentication accuracy; however, other parameters will be included if appropriate.	

In addition, the parameters of the operational environments to be studied will be articulated.

5.2 Select Biometric Products for Evaluation

Using a methodology similar to that used to select BCA topics, the DHIAP Team will assess the available technologies/products and identify at least four biometric products representative of the currently available technologies for evaluation in this task. Since product selection will consider those products approved/recommended by the DOD

Biometrics Management Office (BMO), this activity will also initiate coordination with the BMO.

5.3 Develop the Prototype and Data Collection Requirements, Specifications

Based on user requirements, obtained primarily from October and November 2001 meetings with TATRC, technology assessment, and product selection, the DHIAP Team developed the functional requirements and technical specifications for integrating the biometrics and data collection software (and associated database). The scenario for testing the authentication method will be to unlock a Windows NT/2000 screen saver (i.e., we will set the screen saver for quick activation, forcing the user to re-authenticate by either password[34] or biometric). As such, the Team determined the functional requirements and technical specifications for interfacing with the NT/2000 (screen saver) log-on and the means to capture parametric data. To the maximum extent possible, the DHIAP Team will leverage vendor expertise throughout the development process, and the Team will coordinate with the BMO to ensure the prototype meets applicable DoD standards.

Goal: To study the effects of applying biometric authentication modes in an operational MTF environment in order to determine (1) which biometric is suitable for a given environment, and (2) whether there is evidence to support replacing passwords with biometrics.

5.3.1 Assumptions

- MTFs have in place and enforce a "good" password policy
- The system will not impact upon the MTF network nor upon the MTF systems (e.g., CHCS)
- Password authentication, based upon a good password policy, will be available (as backup, in the event a user is unable to authenticate with a biometric mode)
- Operational environments – those established in BCA, *Effective Authentication in a Medical Environment*, as defined in Activity 5.1
- Notional System Description
    - User re-authentication from screen saver lockout.
        - This assumes that the user has already authenticated to the workstation/network and that the screen saver is set to a short time.
        - Also, the biometric prototype will not begin operation until the screen saver re-authentication is used.
    - Capable of authenticating a user in one of four biometric modes (finger, voice, face, iris) and password in a given operational environment

[34] Note that passwords will always be available to ensure a biometric authentication failure does not unduly interfere with operations.

  - Authentication via verification (user[35] claims an identity and system will verify it), rather than identification (system searches a database for the "best" match)
  - Operating system will be Windows NT or 2000; it is worth noting, however, that Windows XP may deserve consideration as it is reportedly capable of supporting a form of session caching along with biometric authentication
  - Integration via third party software
  - GUI with capability to collect parameters, as described in Activity 5.1, in a local database
  - Biometric Prototype System configuration:
    - **Stage 1**. A PC will be equipped with one biometric mode/device and password for user re-authentication (upon activation of the screen saver). Users will have a choice of re-authenticating with either the biometric or the password. The data collection effort will entail rotating each biometric mode on the PC within each of up to four operational environments.
    - **Stage 2**. A PC will be equipped with up to four biometric modes and password for user re-authentication. The user, having been trained in Stage 1 on each method of authentication, will choose the method of authentication (thereby providing user acceptance data). The data collection effort will entail rotating the PC through each of up to four operational environments. Integration of the biometric modes on one PC will heavily rely upon third party vendors (such as SafLink and BioConeX).
- If demonstrated at ATA, the ATA demonstration prototype will not become a separate development effort; rather, it will support the overall effort
  - ATA demonstration will likely be a multi-modal verification station with a GUI
  - GFE (e.g., masks, gloves, hoods, goggles, etc.) will be provided for ATA demonstration

5.3.2 Functional Capabilities

The first step is to assess the user requirements and determine the functional capabilities. The functional capabilities describe how the system will work and what it should do. The system will consist of two primary components, the GUI and the database.

- GUI Functional Capabilities
  - Prompt the user through the enrollment process
  - Prompt the user on how he/she would like to authenticate (biometric or password, this is built into BioConeX third party package)
  - Provide access to data collected to administrators (DHIAP Team)
- Data Collection Functional Capabilities

[35] In this case, the user is the person who was logged on when the screensaver was invoked.

- Collect data on parameters as defined in Activity 5.1 (some packages have accuracy collection built-in)
    - Hidden (to user) data collection will consist of criteria such as authentication accuracy, time to enroll, time to authenticate, usage rate, etc.
    - Overt (to user) data collection will include a survey instrument to capture criteria relating to parameters such as user acceptance

5.3.2.1 Functional Attributes

The attributes listed below will be considered in the design and development of the biometric prototype. Note that many of the attributes are also related to the data that will be collected to compare the biometric methods as listed in the parameters in Activity 5.1.

- **Availability** – while biometric products may individually cause false rejects of authorized users, the biometric prototype as a whole should not impede authorized users from accessing applications needed to conduct operations in the environment; passwords will be available if the user is unable to authenticate with a biometric method
- **Efficiency** – the biometric prototype should run in a manner that is transparent to the user in terms of workstation resource (storage, memory, CPU) requirements; minimum workstation configuration requirements will be provided in the site installation plan
- **Flexibility** – the biometric prototype design will consider the possible future need to integrate other biometric products
- **Integrity/Security** – the biometric prototype will maintain protection of the data stored/processed on the workstation by not degrading the security features of the workstation; only administrators will be able to view data collected by the biometric prototype and that data will contain no user-specific data
- **Interoperability** – the biometric prototype will not impede the interoperability of other applications
- **Reliability** – the biometric prototype will be fully tested before any site installation and while individual biometric products may fail according to their own reliability capabilities, the biometric prototype as a whole should not fail to the extent that a workstation reboot cannot correct the problem
- **Robustness** – if the individual biometric method of authentication fails to authenticate an authorized user, password authentication (and conceivably other biometric modes) will be available
- **Usability** – some degree of user learning and user enrollment will be required for each biometric method; however, user acceptance will be a key parameter in comparing methods of authentication

5.3.3 Technical Requirements

Technical requirements identify what is technically necessary to support the functional capabilities.

- General Technical Requirements
  - Operating system – Windows NT/2000
  - Integration of biometric modes to the operating system (screen saver authentication)
- GUI Technical Requirements
  - Integration of GUI to screen saver authentication
  - Integration of GUI to biometric modes and/or to the third party software
- Data Collection Technical Requirements
  - Microsoft Access database (with fields defined by the parameters and evaluation criteria identified in Activity 5.1) unless the data is collected in some other readily available and readable form in the third party software, such as a data delimited ASCII text file
  - Integration of the data collection with the biometric modes of authentication
  - Integration of the data collection with password authentication

5.4 Design and Develop the Prototype

The DHIAP Team will design and develop the Biometric Authentication Prototype in a laboratory environment. The prototype will include the integration of the authentication methods to an NT/2000 workstation along with the data collection software and associated database(s).

5.4.1 Develop System and Software Architectural Design

Using the functional and technical requirements from Activity 5.3, the Team will develop a coordinated top-level design for the technical components of the Biometric Prototype, including, as required:

- GUI design with draft of screen format to be used;
- Design for the local database (e.g., length of field, alpha vs. numeric input, range of acceptable values, etc.) for collecting data;
- Design for the interfaces external to the software and between/among the vendor's biometric products;
- Draft user documentation; and
- Preliminary test procedures.

Upon completion of the design, the Team will conduct a design review with TATRC and update the design, as appropriate, based on results of the meeting.

5.4.2 Perform Software Coding, Testing, and Integration

The Team will develop a Biometric Authentication prototype consisting of the GUI, the data collection database, and biometric products interfaces. The effort will include acquisition of the system platforms (i.e., PC workstations), the biometric products, and development tools (if needed). The software components will be coded and integrated using vendors' support tools to the maximum extent possible to reduce development time. Individual software units and product components will be developed and tested prior to integration to ensure that each satisfies its technical requirements. Regression testing of aggregate components will ensure proper functionality of the whole. Included within this activity, user documentation will be updated as required. To the extent possible (i.e., without unduly interfering with the primary effort), the Team will attempt to have completed a demonstrable prototype in time for the American Telemedicine Association conference (June 2002).

5.5 Collect Data in Laboratory Setting

Once the system has been fully tested to ensure it meets technical requirements, the DHIAP Team will confirm proper operation of the system (i.e., that it meets functional requirements) and collect data in a simulated operational environment.

5.6 Recruit a Site

Concurrent with the requirement specification and laboratory development efforts, the DHIAP Team will work with TATRC to identify an appropriate MTF wherein the prototype can be used to capture real-world operational data.[36] Site recruitment will leverage contact for OCTAVE training and support. Site engagement will include a commitment from the site and DHIAP Team resources. In coordination with TATRC and staff of the trial site MTF, the DHIAP Team will demonstrate and evaluate the prototype functionality and make a checkpoint decision to proceed with installation at the MTF.[37]

5.7 Install Prototype at the Site

The DHIAP Team will work with the trial site MTF to develop an installation plan and, based on a checkpoint decision to proceed, will acquire equipment as needed, install and test the prototype in the MTF, and orient MTF personnel on operations (and maintenance, if necessary) of the system.

5.8 Collect Data in Operational Environment

Once the prototype has been fully tested in the operational environment(s) at the MTF test site, the DHIAP Team will allow it to collect data. Since this task is also a proof of concept demonstration, the Team will work with the trial site to conduct prototype

[36] Ideally, the Team will work with a trial site MTF selected by TATRC to collect operational data. Alternatively, if an MTF is not available to meet the schedule, the Team will simulate the operational environment in the laboratory or other non-MTF site such as the digital deployed hospital at TATRC, and collect operational data in that manner.

[37] Note that laboratory Design and Development activity described above will be conducted with full consideration of installation at the MTF test site and all unknowns will be addressed *before* the start of test site installation.

demonstrations and evaluate the authentication methods' capabilities to address information assurance shortfalls.

5.9 Compile Data and Report

Based on the data collected and the demonstration results, the DHIAP Team will draft recommendations for piloting biometric technology to broader use. The Team will develop and deliver a report on the prototype demonstration results and provide the report and any collected data to TATRC for inclusion in RIMR.

Issues / Dependencies

- Engagement of Prototype Site: The government will identify MTFs willing to participate in the Biometric Prototype. The DHIAP Team will assist in briefing MTF leadership regarding the Biometric Prototype and assist in engaging the MTF for participation in the prototype efforts.
- Verification vs. Identification: This study will be based on biometric verification (i.e., a 1::1 match for user authentication), rather than identification (i.e., a 1::many search of possible users).
- Effect of Unknowns on Schedule/Scope of an R&D Effort:
- The collection of truly operational data (i.e., from a medical environment) will be contingent upon recruitment of MTF(s) to participate in the task; however, useful data resulting from independent biometric laboratory testing and evaluation will be captured regardless of whether an MTF is recruited.
- Unforeseen operational requirements (e.g., deployment) at the test site MTF may interrupt the schedule of installation, data collection, and prototype demonstration at the test site.
- The development of the Biometric Prototype is a research and development task. The objective of the effort is to design, develop, prototype, test, and install a prototype system of biometric authentication methods for data collection and authentication analysis. Biometrics is an area of emerging technology, lacking standards in development and testing (and not all products may be compliant with the Biometric Application Programming Interface [BioAPI]), thereby bringing a degree of risk to the accomplishment of successfully developing an operational prototype.
- GFE for ATA Conference: The Team may require use of items such as surgical gloves, masks, hoods, loupes, etc. to support the demonstration at the ATA Conference.

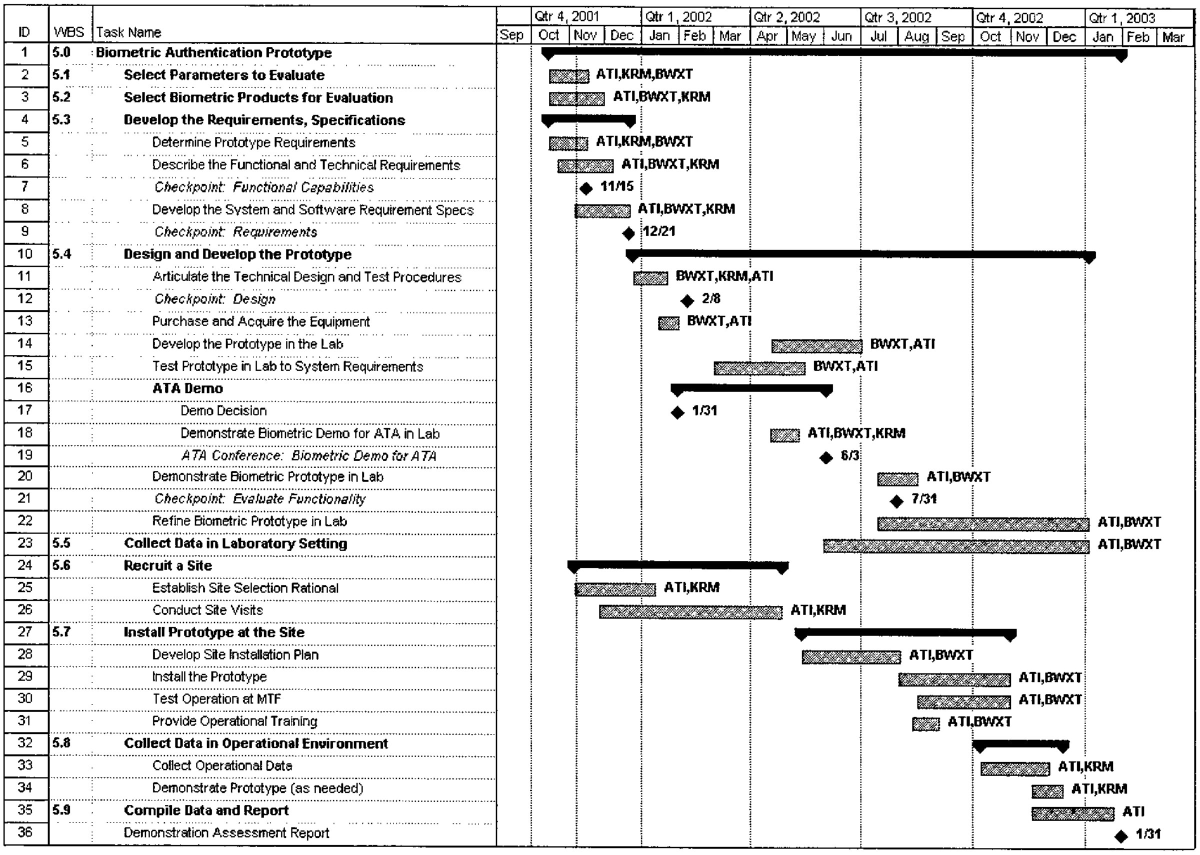
Deliverables

- Implementation plan for a representative pilot MTF as an addendum to the TDP
- Prototype demonstration in a laboratory environment
- Prototype installation at the MTF and staff training on prototype use and support
- If appropriate, transition of the prototype to operations
- Lessons Learned Report on demonstration evaluation

DHIAP Phase III Technical Development Plan

Schedule

Figure 9 below indicates the activities, planned timeframes, and participants of the major activities of the Biometric Prototype effort.



ID	WBS	Task Name
1	5.0	**Biometric Authentication Prototype**
2	5.1	**Select Parameters to Evaluate**
3	5.2	**Select Biometric Products for Evaluation**
4	5.3	**Develop the Requirements, Specifications**
5		Determine Prototype Requirements
6		Describe the Functional and Technical Requirements
7		*Checkpoint: Functional Capabilities*
8		Develop the System and Software Requirement Specs
9		*Checkpoint: Requirements*
10	5.4	**Design and Develop the Prototype**
11		Articulate the Technical Design and Test Procedures
12		*Checkpoint: Design*
13		Purchase and Acquire the Equipment
14		Develop the Prototype in the Lab
15		Test Prototype in Lab to System Requirements
16		**ATA Demo**
17		Demo Decision
18		Demonstrate Biometric Demo for ATA in Lab
19		*ATA Conference: Biometric Demo for ATA*
20		Demonstrate Biometric Prototype in Lab
21		*Checkpoint: Evaluate Functionality*
22		Refine Biometric Prototype in Lab
23	5.5	**Collect Data in Laboratory Setting**
24	5.6	**Recruit a Site**
25		Establish Site Selection Rational
26		Conduct Site Visits
27	5.7	**Install Prototype at the Site**
28		Develop Site Installation Plan
29		Install the Prototype
30		Test Operation at MTF
31		Provide Operational Training
32	5.8	**Collect Data in Operational Environment**
33		Collect Operational Data
34		Demonstrate Prototype (as needed)
35	5.9	**Compile Data and Report**
36		Demonstration Assessment Report

Figure 9 – Schedule for the Biometric Prototype Effort

Travel

Most travel for this project involves site coordination among the DHIAP Team members and between the DHIAP Team and the MTF test site. Note that the sites identified in the travel "To" destinations in the table below are listed for budget estimation purposes only; the intent is to minimize travel costs by designating a site within easy surface transport from Charleston SC. Projected travel is depicted in Table 5 below. Note that the Team Members column indicates "(TATRC)" for trips involving meetings in which the TATRC team members may wish to participate. This information is provided for TATRC's budgeting of potential travel.

Table 5 - Proposed Travel for Biometric Prototype

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Nov-01 B1	Washington, DC w/ M5, T4, O2	Functional Capabilities check with TATRC Checkpoint on Requirements and Specifications with TATRC	ATI, BWXT, KRM	3

Month Trip #	To	Reason	Team Member(s)	Contractor Travelers
Jan-02 B2	Charleston, SC w/ M6, T5, O4	Project Coordination for Design Checkpoint on Prototype Design with TATRC	ATI or BWXT, KRM	2
Mar-02 B3	Charleston, SC w/ O6	Project Coordination for Development	ATI or BWXT, KRM	2
Apr-02 B4 (Optional)	Charleston, SC	Demonstrate Biometric Demo for ATA in Lab	BWXT, KRM (TATRC)	2
Jun-02 B5 (Optional)	Los Angeles, CA	Demonstrate Biometric Demo at American Telemedicine Association 2002 conference	ATI, BWXT, KRM (TATRC)	3
Jul-02 B6	Charleston, SC w/ O8	Demonstrate Lab Prototype and Checkpoint on Functionality	BWXT, KRM, (TATRC, MTF Reps)	2
Aug-02 B7 (Optional)	Ft. Bragg, Fayetteville, NC	Install and Test Prototype at MTF	ATI, BWXT	3
Oct-02 B8 (Optional)	Ft. Bragg, Fayetteville, NC	Site Installation follow-up at MTF	ATI, BWXT	3
Nov-02 B9 (Optional)	Ft. Bragg, Fayetteville, NC	Gather Data for Report on Demonstration Results at MTF	ATI, KRM, (TATRC)	2

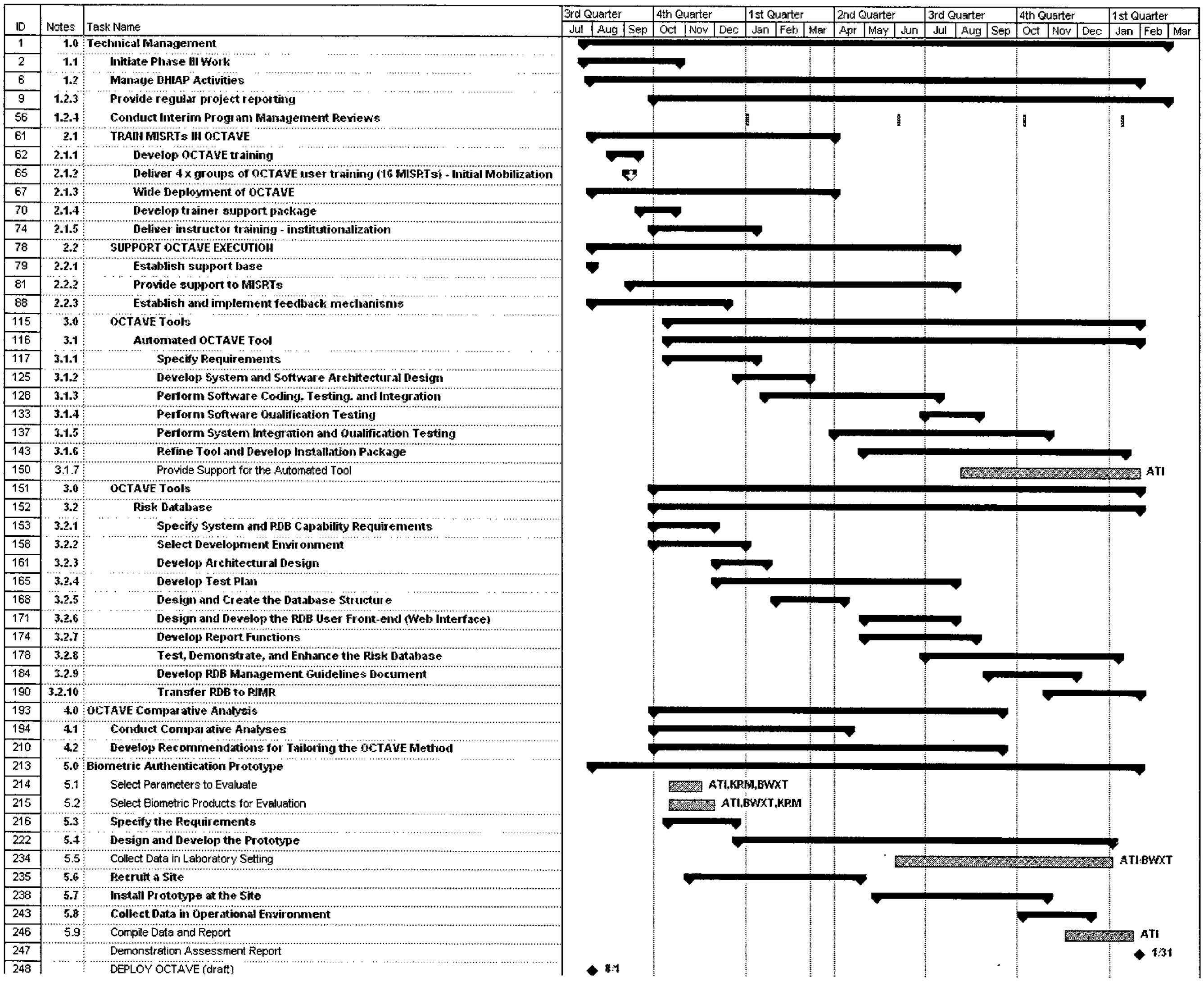
Equipment

The equipment requirements to support this task are the biometric products (e.g., scanner and software) to be included in the prototype. Since the actual product(s) to be purchased for this effort will not be determined until the Functional Requirements, Technical Specifications, and Product Selection activities have been completed (Major Activities 5.2 and 5.3), examples of each type of equipment are presented in Table 6 below.

Table 6 - Example of Materials for Biometric Prototype

Device Type / Source	Product
Finger Scan Recognition	• *DigitalPersona Finger Printer Security, U are U Pro Workstation Systems*

Appendix A to TDP – Detailed Schedule for Phase III Projects



ID	Notes	Task Name
1	1.0	**Technical Management**
2	1.1	**Initiate Phase III Work**
6	1.2	**Manage DHIAP Activities**
9	1.2.3	**Provide regular project reporting**
56	1.2.4	**Conduct Interim Program Management Reviews**
61	2.1	**TRAIN MISRTs IN OCTAVE**
62	2.1.1	**Develop OCTAVE training**
65	2.1.2	**Deliver 4 x groups of OCTAVE user training (16 MISRTs) - Initial Mobilization**
67	2.1.3	**Wide Deployment of OCTAVE**
70	2.1.4	**Develop trainer support package**
74	2.1.5	**Deliver instructor training - institutionalization**
78	2.2	**SUPPORT OCTAVE EXECUTION**
79	2.2.1	**Establish support base**
81	2.2.2	**Provide support to MISRTs**
88	2.2.3	**Establish and implement feedback mechanisms**
115	3.0	**OCTAVE Tools**
116	3.1	**Automated OCTAVE Tool**
117	3.1.1	**Specify Requirements**
125	3.1.2	**Develop System and Software Architectural Design**
128	3.1.3	**Perform Software Coding, Testing, and Integration**
133	3.1.4	**Perform Software Qualification Testing**
137	3.1.5	**Perform System Integration and Qualification Testing**
143	3.1.6	**Refine Tool and Develop Installation Package**
150	3.1.7	Provide Support for the Automated Tool
151	3.0	**OCTAVE Tools**
152	3.2	**Risk Database**
153	3.2.1	**Specify System and RDB Capability Requirements**
158	3.2.2	**Select Development Environment**
161	3.2.3	**Develop Architectural Design**
165	3.2.4	**Develop Test Plan**
168	3.2.5	**Design and Create the Database Structure**
171	3.2.6	**Design and Develop the RDB User Front-end (Web Interface)**
174	3.2.7	**Develop Report Functions**
178	3.2.8	**Test, Demonstrate, and Enhance the Risk Database**
184	3.2.9	**Develop RDB Management Guidelines Document**
190	3.2.10	**Transfer RDB to RIMR**
193	4.0	**OCTAVE Comparative Analysis**
194	4.1	**Conduct Comparative Analyses**
210	4.2	**Develop Recommendations for Tailoring the OCTAVE Method**
213	5.0	**Biometric Authentication Prototype**
214	5.1	Select Parameters to Evaluate
215	5.2	Select Biometric Products for Evaluation
216	5.3	**Specify the Requirements**
222	5.4	**Design and Develop the Prototype**
234	5.5	Collect Data in Laboratory Setting
235	5.6	**Recruit a Site**
238	5.7	**Install Prototype at the Site**
243	5.8	**Collect Data in Operational Environment**
246	5.9	Compile Data and Report
247		Demonstration Assessment Report
248		DEPLOY OCTAVE (draft)

DHIAP Phase III No-Cost Extension Request

Appendix 5 – Revised Program Plan—DHIAP III, 9 December 2002

During execution of Phase III, changes in some MHS operational priorities were the driver for the timing of several critical path Phase III tasks. These changes, in turn, drove modifications to the sequence and staffing plans of other tasks. Because of these changes some work remains to be completed after the planned Phase III end date of 31 January 2003, and an adequate level of program funding remains to complete them by 31 August 2003. We therefore propose extending the period of technical work on Phase III to 31 August 2003 at no additional cost to the government.

The summary below indicates each Phase III project and outlines the nature and basis of each proposed schedule change. A table included with each task write-up lists the tasks that we anticipate will remain to be completed as of 31 January 2003, as well as our plan for completing them by the 31 August 2003 end of a no-cost extension timeframe. Note TATRC has requested that certain of these tasks be continued beyond August 2003 and provided separate funding to support the effort; these tasks' "revised plan" write-up indicate this fact and refer to that funding as OCTAVE Training and Support (OTAS).

Approval of this request for a no-cost extension will allow us to continue support for DHIAP under current funding until the end of August 2003 when OCTAVE Training and Support funding will pick up support costs for military medical OCTAVE users.

1 Technical Management

Status Summary: Technical Management activities have been completed on schedule and according to plan.

Proposed Adjustment to Plan: We propose that activities for management of Phase III continue through completion of the technical activities in August 2003. After that, the task will then remain active (through January 2004) to develop and publish the DHIAP Phase III Final Report. The task that remains open is listed below.

Phase III Subtask	Task Dependency	Revised Plan
1.2 Manage DHIAP Activities	n/a	Extend the effort through September 2003 to support completion of technical activities by 31 August 2003 and delivery of the Final Report in September 2003.

2 Deploy OCTAVE

2.1 Train MISRTs on OCTAVE

Status Summary: This task's activities to develop and execute MISRT training have been completed, and its development and documentation of a Train-the-Trainer Seminar will be completed by 31 March 2003.

Proposed Adjustment to Plan: Because the service organization(s) that will be the military's ongoing provider of MISRT training has not been identified, it is not likely that the portions of the effort relating to turning over a training course and training responsibility to a DOD-designated service organization will have been completed by the end of Phase III. Tasks remaining open are listed below.

Phase III Subtask	Task Dependency	Revised Plan
2.1.4 Identify DOD Trainers (support TATRC)	n/a	Rather than concentrating on identifying the specific DOD trainers, we will revise Task 2.1.5 to produce a generic instructor's package suitable for most DOD trainers.
2.1.5 Deliver Instructor Training Package to DOD	Task 2.1.4	The portion of this effort that develops a Train-the-Trainer Instructor's Package will be complete in March 2003. ATI will adapt the Train-the-Trainer course for the military, reflecting the changes made to the baseline OCTAVE training that was previously adapted for the military. It is anticipated that a service training organization will not have been identified, and therefore the Train-the-Trainer course will be modified in a way that is general enough for all three services to subsequently use.

2.2 Support OCTAVE Execution

Status Summary: This task's initial development of a support base, the OCTAVE Information Center (OIC), and associated feedback mechanisms have been completed. The web-enabled OIC provides a forum for OCTAVE users in the field to access and download OCTAVE-related documentation and to request assistance and receive expert advice from OCTAVE trainers. Through the OIC, the DHIAP Team is providing support to MISRTs as they execute OCTAVE at their sites. The ongoing support for the OIC, planned as a deliverable for this task, is being provided on schedule.

Proposed Adjustment to Plan: Since MISRT training was deferred from the original September 2001-January 2002 plan to May-August 2002, this task's activities to continue to support trained MISRTs should be extended beyond the original planned timeframe in order to meet the original expectation of helping DOD MTFs complete execution of their OCTAVEs. The activities proposed to be conducted during the requested Phase III extension period include providing support to the trained MISRTs while they execute OCTAVEs at their sites, gathering input from MISRTs about sites' progress in conducting OCTAVEs, and regularly providing MHS/TATRC with reports of site progress. The task that remains open is listed below.

Phase III Subtask	Task Dependency	Revised Plan
2.2.2 Provide Support to MISRTs	Task 2.1.3	We propose to extend the time period for providing support to MISRTs for the duration of the requested extension, through 31 August 2003; ATI will perform the work of this task. (Note that continuation of these efforts beyond August 2003 is included in the DHIAP-related OTAS funding, in that effort's "Support OCTAVE Execution" task.)

3 OCTAVE Tools

3.1 OCTAVE Automated Tool

Status Summary: The OCTAVE Automated Tool (Tool) was developed, tested by ATI and SEI, and provided to TATRC and MHS for review, testing, and comment. Feedback from the various levels of testing and some limited public exposure was used to enhance the Tool and

DHIAP Phase III No-Cost Extension Request

produce a Beta version. The Beta release was tested by ATI, provided to SEI for additional testing, and offered to MISRTs that had attended OCTAVE MISRT training for their use in the field while conducting their sites' OCTAVEs. As planned, the developers will support the military "field" users of the Tool through the scheduled end of Phase III and collect/document suggestions for Tool enhancement.

Proposed Adjustment to Plan: We propose augmenting the scheduled tasks in Phase III to continue the support and enhancement of the Automated Tool during its early Beta version use by MISRTs. Since the Tool is used by a number of military field users as the repository for data they collect during execution of their OCTAVEs, this task will provide the basis for (1) supporting an extended beta test of the Tool if deemed necessary, (2) identifying essential Tool enhancements based on feedback provided during field use, and (3) updating the Beta version to include the selected enhancements. The tasks that would be completed as part of the extended effort are listed below.

New Task/Subtask	Task Dependency	Revised Plan
New 3.1.7-3.1.11 Additional Automated Tool Effort	n/a Extension of Tasks 3.1.6 and 3.1.7	We propose conducting this effort (subtasks listed below) from February through June 2003.
Extend 3.1.7 Support Extended Beta Test of OCTAVE Automated Tool	Task 3.1.7	Continuation of Phase III Task 3.1.7. In addition to providing Tool-related assistance and advice to field users, ATI will collect field users' comments and suggestions about the Beta version of the Tool. If an updated version of the Beta Tool is developed and released (see 3.1.9 below), this task will provide user support for that version. The task will be performed from February through June 2003. (Note that continuation of this effort beyond June 2003 is included in the DHIAP-related OTAS funding, in that effort's "Support OCTAVE Execution" task.)
New 3.1.8 Select Enhancements from Support Feedback	Task Revised 3.1.7	ATI will evaluate the field users' comments and suggestions about the Beta version of the Tool, classify and prioritize them, and use this information to determine enhancements that should or must be made to the Tool. This activity will be performed in February 2003.
New 3.1.9 Code Enhancements to Beta Tool	Task New 3.1.8	ATI will implement the selected enhancements in the currently fielded Beta version of the Tool and perform developer testing to assure they work as designed. If these are significant changes to the operation or functionality of the tool, a second Beta release may be appropriate; otherwise, the code enhancements will result in the production version. This activity will be performed on in March immediately following completion of related Task 3.1.8 activity.
New 3.1.10 Test Production and Release to Field for Acceptance	Task New 3.1.9	ATI will thoroughly test the updated Tool and, when complete, make the updated version available to MISRTs in the field for their use. This activity will be performed in April 2003. Testing will include security testing and preparing appropriate documentation to a standard and in a format that would be expected for submission to a DAA for a C&A designation of Interim Authority to Operate (IATO). Individuals within the program who have been independent of the tool development will perform the required testing and

		documentation. Testing of the OAT will be performed independently of RDB testing in order that it may be released as a stand-alone tool for MTFs to use as they begin execution of their OCTAVE. Final security testing for the OAT and RDB together as a system will be completed prior to completion of DHIAP III and subsequently transitioned to the DOD.
New 3.1.11 Support Production version of OCTAVE Automated Tool	Task New 3.1.10	With the fielding of the production version of the tool, support will be under configuration control. Desired and required changes to the tools functionality will be managed as engineering change proposals (ECP). Revisions to the tools will be scheduled at regular intervals dependent on nature and impact of ECPs.

3.2 Risk Database

Status Summary: The Risk Database (RDB) was developed and is currently undergoing testing, according to schedule. Also, a set of standard reports were developed and tested, and development of documentation for supporting and using the RDB has been initiated.

Proposed Adjustment to Plan: The RDB is the repository for data captured during sites' execution of OCTAVE. Since the sites began executing their OCTAVEs several months later in Phase III than had originally been planned (due to the deferral of MISRT training), very little data will have actually been provided to the RDB by the time Phase III ends, and there will have been little opportunity to fine-tune the RDB based on results of its working with data provided from the field. Therefore, we propose extending the timeframe of certain activities to allow them to improve their deliverables based on working with field data. We have also added a new task to support the RDB's users (e.g., MHS or TATRC analysts who will work with, or simulate working with, the field-provided data and the TATRC systems administrators who will assume the responsibilities of user-liaison and support staff for the RDB). The tasks remaining open and the new task are listed below.

Phase III Subtask	Task Dependency	Revised Plan
3.2.7 Develop Report Functions	Tasks 3.2.6, 3.2.8	Each of the Phase III subtasks 3.2.7 through 3.2.9 was partially completed during the scheduled timeframe of Phase III. However, since very few field users of the Beta OCTAVE Automated Tool are likely to have completed their site OCTAVEs and transferred the resulting data from the Tool to the RDB by the end of Phase III, in-depth testing of RDB functionality and reporting, as well as realistic use of its management/support instructions, will not be possible. We propose to
3.2.8 Test, Demonstrate, and Enhance the Risk Database	Task 3.2.6	

3.2.9 Develop RDB Management Guidelines Document	Tasks 3.2.6, 3.2.8	management/support instructions, will not be possible. We propose to extend the work of these tasks through June 2003 in order to incorporate into these Phase III deliverables any lessons learned from populating the RDB with field data. Testing will include security testing and preparing appropriate documentation to a standard and in a format that would be expected for submission to a DAA for a C&A designation of Interim Authority to Operate (IATO). Individuals within the program who have been independent of the RDB development will perform the required testing and documentation. Testing of the RDB will be performed independently of OAT testing in order that it may be released as a stand-alone tool for the DOD to use. Final security testing for the OAT and RDB together as a system will be completed prior to completion of DHIAP III and subsequently transitioned to the DOD.
3.2.10 Transfer RDB to RIMR	Task 3.2.9	Execution of this task is dependent upon completion of tasks 3.2.7 through 3.2.9. We propose deferring completion of the task until after completion of new Task 3.2.11 below.
New 3.2.11 Support Beta Test of RDB	Tasks 3.2.6, 3.2.8	This effort will provide assistance and advice to RDB users—both field users transferring data to the RDB and central (e.g., TATRC) users who are reporting and analyzing the data. We will collect the users' comments and suggestions about RDB functionality, determine changes that should or must be made to the software, and work with appropriate users as necessitated by the changes. The task will be performed from February through August 2003. (Note that continuation of this effort beyond August 2003 is included in the DHIAP-related OTAS funding, in that effort's "Support OCTAVE Execution" task.)

4 Comparative Analysis

Status Summary: Developing and publishing OCTAVE comparison reports on DITSCAPwill have been completed during the planned timeframe for Phase III work. During the Phase III period of performance, ATI requested and the COTR agreed that the planned comparison report for RFC 2196 be changed to a comparison against the NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems."

Proposed Adjustment to Plan: We propose extending the timeframe for the last of the planned comparison reports (the first task below) into the period of the no-cost extension. The second task proposed for extension involves preparing recommendations for enhancing OCTAVE for MHS use. Extension of this task is necessary because input to the report consists of information that will be provided as a result of the sites' completion of OCTAVEs (their questions, their problems), a process that we expect will continue through April-May 2003 as the sites complete the OCTAVEs. The tasks remaining open are listed below.

Phase III Subtask	Task Dependency	Revised Plan
4.1.3-5 HIPAA Security, JCAHO, and NIST Standards Comparison Report	n/a	Extend the effort through May 2003.
4.2 Develop Recommendations for Tailoring OCTAVE	Task 2.2.2	Execute the task in April-June 2003, following receipt of comments from sites that completed executing OCTAVEs.

5 Biometric Authentication Prototype

Status Summary: The prototype has been developed and tested, and has been installed for demonstration at the trial site, Naval Hospital Charleston (NHC). All planned task activities will be finished by the February 2003 end of Phase III, with the exception of the demonstration's final report. NHC staff has offered to support considerable flexibility in the places and types of staff that would be part of the demonstration, and we would like to extend the timeframe of the work conducted at NHC to take full advantage of that expanded opportunity.

Proposed Adjustment to Plan: We propose extending the deadline for delivery of the demonstration final report to March 2003 in order to let the demonstration at Naval Hospital Charleston run for as long as possible (e.g., through February 2003). The task that remains open is listed below.

Phase III Subtask	Task Dependency	Revised Plan
5.9 Compile Data and Report	Task 5.8	Extend the effort through March 2003.

Contract No: DAMD17-01-C-0048

Defense Healthcare Information Assurance Program (DHIAP)

Principal Investigator: Archie Andrews
843-760-4537
Advanced Technology Institute
5300 International Blvd.
N. Charleston, SC 29418

Reporting Period from 30 July 2001 to 15 August 2003

31 August 2003

Addendum to Final Report: DHIAP Phase III

ATI IPT 03-09

Prepared for:
U.S. Army Medical Research and Materiel Command
Fort Detrick
Frederick, Maryland 21702-5012

Table of Contents

Table 1: DHIAP Phase III Publications and Presentations

Date	Presentation / Publication	For
24 October 2002	Share OCTAVE/DHIAP Information **Presenters:** ATI	HIPAA Privacy Rules Seminar in Columbia SC
18-21 February 2003	Present DHIAP Research **Presenters:** ATI	SPIE Medical Imaging 2003 Conference in San Diego CA
28-30 April 2003	Present DHIAP Research **Presenters:** ATI	American Telemedicine Association 2003 Conference in Orlando FL

Table 2: DHIAP Phase III Significant Meetings

Date	Meeting Abstract	Location
2 August 2001	Phase III planning **Participants:** ATI, SEI, TATRC	Washington DC
21-23 August 2001	Confirm the group approach to HIPAA Summit training **Participants:** ATI, KRM, TATRC, SEI	Pittsburgh PA
4-7 September 2001	Conduct HIPAA Summit OCTAVE training **Participants:** ATI, KRM, TATRC, SEI	Arlington, VA
12-14 September 2001	Review Phase III proposal commitments/plan initial TDP development activities **Participants:** ATI, KRM, BWXT	Charleston SC
15-18 October 2001	Discuss/confirm TDP contents, discuss each project's initial deliverables **Participants:** ATI, TATRC, KRM, SEI, BWXT, ADL	Charleston SC
13-14 November 2001	Review technical designs, training plans **Participants:** ATI, TATRC, SEI, KRM	Ft. Detrick MD
15-17 January 2002	Review project status, technical designs, training plans **Participants:** ATI, KRM, BWXT Y-12 LLC, SEI, ADL Visitors: representatives from Naval Hospital Charleston; demo conference call with BioNetrix	Charleston SC
7-8 February 2002	Technical review of RDB architecture and design **Participants:** KRM, SEI	Pittsburgh PA
6-7 March 2002	Review OCTAVE Tools Architecture, designs, software prototype; review Biometric Prototype requirements, plans, vendor capabilities **Participants:** ATI, KRM, BWXT Y-12 LLC, TATRC, ADL Visitors: representative from Naval Hospital Charleston; representatives from BioNetrix	Charleston SC
12 March 2002	Review ***program status and progress*** with COTR at TATRC **Participants:** TATRC, ATI	Ft. Detrick MD
29-31 January 2002	Attend OCTAVE training at SEI **Participants:** ATI	Pittsburgh PA
7-8 February 2002	Technical review of RDB architecture and design **Participants:** KRM, SEI	Pittsburgh PA
15-16 April 2002	Deliver and present Alpha version of OCTAVE Automated Tool for usability testing **Participants:** ATI, SEI, TATRC	Ft. Detrick MD and Pittsburgh PA
9-10 May 2002	Gather team members who will conduct OCTAVE Training, complete planning for logistics/travel/training, review lesson plans/delivery approach **Participants:** TATRC, KRM, ATI	Charleston SC
16 May 2002	Discuss SEI feedback on usability testing of OCTAVE Automated Tool **Participants:** SEI, ATI	Charleston SC

Date	Meeting Abstract	Location
10-11 July 2002	Region 1 OCTAVE Training **Participants:** ATI, KRM, TATRC	Washington DC
15-16 July 2002	Region 10 OCTAVE Training **Participants:** ATI, TATRC	Sacramento CA
16-17 July 2002	Region 5 OCTAVE Training **Participants:** ATI, TATRC	Dayton OH
18-19 July 2002	Region 9 OCTAVE Training **Participants:** ATI, TATRC	San Diego CA
22-23 July 2002	Region 12 OCTAVE Training **Participants:** ATI, TATRC	Honolulu HI
24-25 July 2002	Region 3 OCTAVE Training **Participants:** ATI, TATRC	Augusta GA
6-7 August 2002	Regions 7 & 8 OCTAVE Training **Participants:** ATI, TATRC	Colorado Springs CO
13-14 August 2002	Makeup OCTAVE Training **Participants:** ATI, TATRC	Washington DC
15-16 August 2002	Region 12 OCTAVE Training **Participants:** ATI, TATRC	Yokota, Japan
19-20 August 2002	Region 11 OCTAVE Training **Participants:** ATI, TATRC	Seattle-Tacoma WA
21 August 2002	Reviewed status of RDB development and completed design for OAT-RDB data transfer **Participants:** ATI, KRM	Charleston SC
22 August 2002	Conducted Biometric verification demonstration; discussed configuration options and timeframe for data collection plan at Naval Hospital Charleston **Participants:** ATI, KRM, Naval Hospital Charleston	Charleston SC
10 September 2002	Meet with team members who will participate in OCTAVE demonstration, complete planning for logistics/travel/training, review lesson plans/delivery approach **Participants:** ATI, Naval Hospital Charleston	Charleston SC (at Naval Hospital Charleston)
19-20 September 2002	Attend OCTAVE Users Forum and receive Train-the Trainer Package updated materials from SEI **Participants:** ATI, KRM, SEI, TATRC	Arlington VA
13-14 October 2002	Present DHIAP and OCTAVE to North Carolina Healthcare Information and Communications Alliance at annual conference **Participants:** ATI	Asheville NC
24 October 2002	Attend HIPAA Privacy Rules Seminar and share OCTAVE/DHIAP Information **Participants:** ATI	Columbia SC
12-14 February 2003	Attend "Train-the Trainer" and OCTAVE-S training at SEI **Participants:** ATI	Pittsburgh PA

Date	Meeting Abstract	Location
18-21 February 2003	Present DHIAP Research at SPIE Medical Imaging Conference **Participants:** ATI	San Diego CA
3-4 April 2003	SEI visit to ATI for OCTAVE-S discussions and presentations **Participants:** ATI, SEI	Charleston SC
28-30 April 2003	Present DHIAP Research at ATA 2003 **Participants:** ATI	Orlando FL
8 May 2003	DHIAP Team Meeting at ATI for OAT-RDB Demonstrations and OCTAVE-S Overview **Participants:** ATI, TATRC, KRM	Charleston SC

Table 3: Personnel Receiving Pay from DHIAP Phase III

Name	Company
Archie Andrews	Advanced Technology Institute
Patricia Austin	Advanced Technology Institute
Bryan Bryant	Advanced Technology Institute
Andrea Caraway	Advanced Technology Institute
Johnathan Coleman	Advanced Technology Institute
Lynn Crane	Advanced Technology Institute
Sarah Hartline	Advanced Technology Institute
Rebecca Hood	Advanced Technology Institute
Lane Melton	Advanced Technology Institute
Steve Pellissier	Advanced Technology Institute
Melanie Ridenhour	Advanced Technology Institute
Robert Scudder	Advanced Technology Institute
Jack Stinson	Advanced Technology Institute
Wanda Torres	Advanced Technology Institute
Wayne Wilcher	Advanced Technology Institute
Becky Ball	BWXT Y-12, LLC (formerly LMES)
Carla Decker	BWXT Y-12, LLC (formerly LMES)
Steve Packard	BWXT Y-12, LLC (formerly LMES)
Forest Schwengels	BWXT Y-12, LLC (formerly LMES)
Kibbee Streetman	BWXT Y-12, LLC (formerly LMES)
Chris Alberts	Software Engineering Institute
Julia Allen	Software Engineering Institute
Jose Caldera	Software Engineering Institute
Audrey Dorofee	Software Engineering Institute
David Fisher	Software Engineering Institute
Kevin Houle	Software Engineering Institute
Suresh Konda	Software Engineering Institute
John Kochmar	Software Engineering Institute

DHIAP Phase III Technical Development Plan

Device Type / Source	Product
http://www.digitalpersona.com	• *DigitalPersona Finger Printer Security, U are U Software Development Kit (SDK), Platinum Edition*
Voice Recognition http://www.verivoice.com	• *VeriVoice Security Lock (SL)* • *VeriVoice SL SDK*
Face Recognition http://www.visionics.com	• *FaceIt Screen Saver OEM Module* • *FaceIt NT Eval* • *Verification SDK*
Iris Recognition http://www.iridian.com	• *Authenticam with PrivateID software* • *SDK*
Multi-modal Recognition http://www.bioid.com	• *BioID* • *SDK*
Collection Platform http://www.dell.com	• *Windows NT/2000, Pentium V workstation with 128 MB RAM and 20 GB hard drive* • *For FaceIt: Video for Windows compatible video capture system, either Parallel Port Digital Video Camera, USB Digital Video Camera, ISA or PCI video capture card with compatible camera* • *For FaceIt: Either Microsoft Visual C++ 6.0 or above, Microsoft Visual Basic 5.0 or above, Borland Delphi 5.0 or above*

Participant Roles

This task will be led by ATI, augmented as required by BWXT Y-12 LLC and KRM Associates.

- **ATI** will provide project management and serve as technical lead.
- **BWXT** Y-12 will provide biometric and information assurance technical expertise. Their team members will draw on their expertise to assist in design, development, testing, and installation. BWXT Y-12 will lead the systems integration effort.
- **KRM Associates** will provide support as needed throughout the project, particularly during development of functional requirements.

Name	Company
Howard Lipson	Software Engineering Institute
James McCurley	Software Engineering Institute
David Mundie	Software Engineering Institute
Rich Pethia	Software Engineering Institute
Jan Philpot	Software Engineering Institute
Robert Rosenstein	Software Engineering Institute
Brad Willke	Software Engineering Institute
Bill Wilson	Software Engineering Institute
Patrick Pearcy	South Carolina Research Authority
Patricia Austin	Arthur D. Little, Inc.
Kelly Pennington	Arthur D. Little, Inc.
Thornton White	Arthur D. Little, Inc.
Keith McCall	KRM Associates, Inc.
Patricia Wise	CPRI-HOST